210-CD-001-002

EOSDIS Core System Project

Risk Assessment Report for the ECS Project

Final

March 1995

Hughes Applied Information Systems
Landover, Maryland

Risk Assessment Report for the ECS Project

Final

March 1995

Prepared Under Contract NAS5-60000
CDRL Item 030

SUBMITTED BY

Mark Settle /s/ for 3/22/95

Marshall A. Caplan, Project Manager Date
EOSDIS Core System Project

Hughes Applied Information Systems
Landover, Maryland

210-CD-001-002

This page intentionally left blank.

Preface

This document is a formal contract deliverable with an approval code of 3. This document is delivered to the National Aeronautics and Space Administration (NASA) for information only, but is subject to approval as meeting contractual requirements.

Once approved, this document shall be under the control of the System Integration and Planning Office. Any questions should be addressed to:

Data Management Office
ECS Project Office
Hughes Applied Information Systems
1616 McCormick Dr.
Landover, MD 20785

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Final
iii through xiv	Final
1-1 and 1-2	Final
2-1 through 2-4	Final
3-1 through 3-12	Final
4-1 through 4-10	Final
5-1 through 5-16	Final
6-1 through 6-4	Final
7-1 through 7-24	Final
8-1 through 8-4	Final
9-1 and 9-2	Final
AB-1 through AB-6	Final

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
210-CD-001-002	Final	March 1995	

This page intentionally left blank.

Contents

Preface

1. Introduction

1.1 Identification 1-1

1.2 Scope 1-1

1.3 Purpose 1-2

1.4 Status and Schedule 1-2

1.5 Organization 1-2

2. Applicable Documents

2.1 Parent Document 2-1

2.2 Applicable Documents 2-1

2.3 Information Documents 2-2

3. ECS Technical and Programmatic Context

3.1 ECS Architecture 3-1

3.2 ECS Development Approach and Schedule 3-1

3.3 Interaction of Risks and Project Development Activities 3-3

3.3.1 Risks and the Requirements Process 3-3

3.3.2 Information Engineering Practice Risks 3-5

3.3.3 Reducing Information Engineering Risk 3-6

3.3.4 Interface Control 3-7

3.3.5 Configuration Control Board 3-8

3.3.6 Product Assurance 3-8

3.3.7 Cost Control and Personnel 3-9

4. ECS Risk Management

4.1 ECS Risk Management Panel 4-1

4.1.1 Introduction 4-1

4.1.2 Risk Management Panel Members and Responsibility 4-1

4.1.3 Risk Management Panel Process 4-1

4.1.4. Risk Planning Quality Checklist 4-4

4.2 ECS Risk Management Process 4-4

4.2.1 Introduction to the Risk Process 4-4

4.2.2 Risk Identification 4-4

4.2.3 Risk Estimation 4-6

4.2.4 Risk Evaluation 4-6

4.2.5 Risk Planning 4-9

4.2.6 Risk Control 4-9

4.2.7 Risk Monitoring 4-9

5. Major Risk Mitigation Activities

5.1 Introduction to ECS Risk Mitigation 5-1

5.2 Prototypes and Studies 5-1

5.2.1 Nature of Prototyping 5-2

5.2.2 Prototyping and Risk Reduction 5-3

5.2.3 Prototyping Risk in Tool Selection 5-3

5.2.4 Reducing Prototyping Risk 5-5

5.3 System Modeling 5-5

5.3.1 Nature of Modeling 5-5

5.3.2 Modeling During Development 5-6

5.3.3 Modeling Risk in Tool Selection 5-7

5.3.4 Risk Reduction Through Modeling 5-7

5.4 System Evolvability Tests 5-8

5.4.1 Nature of Evolutionary Packaging 5-8

5.4.2 Risk Reduction Through Evolutionary Packaging 5-8

5.5 Data Modeling 5-8

5.6 Data Migration 5-8

5.7 Interface Management 5-10
5.8 Project Software Development Activities 5-10
5.8.1 Development Environment 5-10
5.8.2 Modeling Activities Versus Schedule 5-11
5.9 Technology Assessment 5-12
5.9.1 Nature of Technology Assessment 5-12
5.9.2 Risk Reduction Through Technology Assessment 5-13
5.10 Object-Oriented Design 5-13
5.11 Software Optimization 5-13
5.12 Integration and Testing 5-14
5.12.1 Testbed 5-14
5.12.2 Independent Acceptance Test Organization 5-14
5.13 ECS Project Cost and Schedule Simulation Model 5-15

6. Risk Identification and Estimation

6.1 Risk Taxonomy 6-1
6.1.1 User Interaction Risks 6-1
6.1.2 Architectural Risks 6-1
6.1.3 Technological Risks 6-1
6.1.4 Evolutionary Risks 6-1
6.1.5 System Operational Risks 6-2
6.1.6 Programmatic Risks 6-2
6.2 Comprehensive Risk Identification 6-2
6.3 Estimation Process 6-2
6.3.1 Interview Process 6-2
6.3.2 Scoring 6-2
6.3.3 Isometric Risk Plot 6-2
6.4 Identified Priority Risks 6-3

7. Priority Risk Evaluation

7.1 Compressed Development Schedule, (P-3) 7-7
7.1.1 Risk Description 7-7
7.1.2 Evaluation Criteria 7-7
7.1.3 Risk Mitigation Plans 7-7
7.1.4 Contingency Plans 7-8
7.2 Operations Concept and Multi-Segment Integration, (P-7) 7-9
7.2.1 Risk Description 7-9
7.2.2 Evaluation Criteria 7-9
7.2.3 Risk Mitigation Plans 7-10
7.2.4 Contingency Plans 7-10
7.3 COTS Full Lifecycle Cost and Management, (A-6) 7-11
7.3.1 Risk Description 7-11
7.3.2 Evaluation Criteria 7-11
7.3.3 Risk Mitigation Plans 7-11
7.3.4 Contingency Plans 7-12
7.4 CSMS Service by Platform, (T-11) 7-12
7.4.1 Risk Description 7-12
7.4.2 Evaluation Criteria 7-13
7.4.3 Risk Mitigation Plans 7-13
7.4.4 Contingency Plans 7-13
7.5 Communication Service System Performance Overhead, ... 7-14
7.5.1 Risk Description 7-14
7.5.2 Evaluation Criteria 7-14
7.5.3 Risk Mitigation Plans 7-14
7.5.4 Contingency Plans 7-15
7.6 COTS Hierarchical Storage Management, (T-4) 7-15
7.6.1 Risk Description 7-15
7.6.2 Evaluation Criteria 7-16
7.6.3 Risk Mitigation Plans 7-16
7.6.4 Contingency Plans 7-16

7.7 Cost-Effective Storage Technology, (T-5) 7-16
7.7.1 Risk Description 7-16
7.7.2 Evaluation Criteria 7-17
7.7.3 Risk Mitigation Plans 7-17
7.7.4 Contingency Plans 7-17
7.8 Archive Scalability and Maintainability, (T-8) 7-18
7.8.1 Risk Description 7-18
7.8.2 Evaluation Criteria 7-18
7.8.3 Risk Mitigation Plans 7-18
7.8.4 Contingency Plans 7-18
7.9 Number and Activity of Users, (U-1) 7-19
7.9.1 Risk Description 7-19
7.9.2 Evaluation Criteria 7-19
7.9.3 Risk Mitigation Plan 7-19
7.9.4 Contingency Plans 7-20
7.10 Production Planning and Scheduling, (S-7) 7-20
7.10.1 Risk Description 7-20
7.10.2 Evaluation Criteria 7-20
7.10.3 Risk Mitigation Plans 7-20
7.10.4 Contingency Plans 7-21
7.11 Database Management Systems, (T-7) 7-21
7.11.1 Risk Description 7-21
7.11.2 Evaluation Criteria 7-21
7.11.3 Risk Mitigation Plans 7-22
7.11.4 Contingency Plans 7-22
7.12 Processing and Storing Standard Products, (U-4) 7-22
7.12.1 Risk Description 7-22
7.12.2 Evaluation Criteria 7-23
7.12.3 Risk Mitigation Plans 7-23
7.12.4 Contingency Plans 7-23

8. Risk Control and Monitoring

8.1 Key Strategic Decisions 8-1
8.2 Integrated Risk Mitigation Plan 8-1
8.3 Risk Monitoring Parameters 8-2

9. Interim Release 1 and Release A

9.1 Conclusions 9-1
9.2 Recommendations 9-1

Abbreviations and Acronyms

Figures

3-1. ECS Development Approach 3-4
4-1. Risk Management Panel Process 4-3
4-2. Risk Management Process 4-5
4-3. Sample Risk Items 4-8
8-1. Key Strategic Decisions Mapped to the Prioritized Risk List 8-2
8-2. Key Strategic Decisions Linked to Program Milestones 8-3
8-3. Integrated Risk Mitigation Plan 8-4

Tables

3-1. ECS Programmatic Risks 3-2
4-1. Risk Management Panel Membership, Roles, and Responsibilities 4-2
4-2. Risk Item Attributes 4-3
4-3. Risk Planning Quality Checklist 4-4
4-4. Consequence of Failure Calculation 4-7
4-5. Probability of Failure Calculation 5-7

4-6. Sample Risk Items 4-8
7-1. Prioritized Risk List 7-2
7-2. Reallocated Risk List 7-2
7-3. Prototypes Mapped to Priority Risk Items 7-3
7-4. Studies Mapped to Priority Risk Items 7-4
7-5. Studies Mapped to Priority Risks - SDPS 7-5
7-6. Studies Mapped to Priority Risks - CSMS 7-6

This page intentionally left blank.

1. Introduction

1.1 Identification

This document is the Interim Release 1 (IR1) of Data Item Description (DID) 210/SE3, Risk Assessment Report, as specified in the Contract Data Requirements List (CDRL) for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS). The next Risk Assessment Report is due at the Incremental Design Review (IDR) minus 2 weeks for each Release.

The Risk Assessment Report shall analyze risks affecting the technical, development, schedule, or cost objectives of the ECS Project, assessing the potential impact of that risk, identifying and analyzing available alternatives, and determining which design alternatives will mitigate or minimize the risk.

This report is about risk and risk mitigation associated with the ECS Project, data and information systems, and ECS Project analysis, design, development, maintenance, and management. The report will help to structure the ECS for success. It has been tailored to assist project managers to plan and manage data and information processing and to deliver the ECS system on time and within budget.

DID 210/SE3 will be updated prior to each IDR. Because the Risk Assessment Report is a living document, questions, comments, and material are and will be continually solicited from team members and the customer. Background materials, including lessons learned and risk/risk mitigation tables, were used extensively to reduce volume. At the Preliminary Design Review (PDR), this report and its attendant parts became part of the ECS development methodology.

ECS is a cost-plus contractual environment where development risk is shared by the customer. Project success and customer satisfaction are ECS goals to be achieved within contractual cost and schedule constraints by implementing the guidelines defined within this report.

1.2 Scope

Risk is inherent to any large-scale, software-intensive system and cannot be avoided. However, risk can be managed to minimize development impact and reduce overall program cost. The techniques described in this document make risk management feasible and effective.

The Risk Assessment Report details the ongoing process and results of risk management as the contractor identifies, evaluates, and eliminates or minimizes inherent or associated ECS Project risks. The Risk Assessment Report provides the results of the ongoing risk identification and analysis process and describes the alternative(s) selected to reduce or eliminate risk elements.

This document reflects the Technical Baseline submitted via contract correspondence number ECS 194-00343.

1.3 Purpose

The purpose of the Risk Assessment Report is to describe for National Aeronautics and Space Administration (NASA) ECS program management the contractor-perceived risk areas as they apply to the tasks identified in the Statement of Work, and to understand how the contractor has identified, assessed, and provided for risk reduction.

1.4 Status and Schedule

This document was initially delivered at PDR minus 2 weeks; this version incorporated any comments following this submission. Subsequent deliveries will be provided at IDR minus 2 weeks for each project Release.

1.5 Organization

The Risk Assessment Report describes the assessment approach, process, and mechanism that the ECS contractor team employs to execute the ECS Statement of Work and other contractual documents. The report serves to: identify, document, and internally assess, milestone by milestone, the risks that will be encountered; and to identify trade studies, prototypes, models, and Evaluation Packages (EP) necessary to make informed management decisions and to mitigate risk well in advance of the event occurrence. The Risk Assessment Report includes the following sections:

a. Section 1, Introduction.

b. Section 2, Applicable Documents. Other parent, related, and information documents are cited.

c. Section 3, ECS Technical and Programmatic Context.

d. Section 4, ECS Risk Management.

e. Section 5, Major Risk Mitigation Activities.

f. Section 6, Risk Identification and Estimation.

g. Section 7, Priority Risk Evaluation.

h. Section 8, Risk Control and Monitoring.

i. Section 9, Interim Release 1 and Release A.

2. Applicable Documents

2.1 Parent Document

The parent document is the document from which this Risk Assessment Report's scope and content derive.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work

2.2 Applicable Documents

The following documents are referenced within this Report, are directly applicable, or contain other directive matters binding upon the content of this volume.

420-05-03	Goddard Space Fight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS)
541-107	NASA Communications (Nascom) Access Protection Policy and Guidelines
NASA-STD-2100-91	NASA Software Documentation Standard, Software Engineering Program
NHB 2410.1D	NASA Handbook: Privacy and Security for Automated Information Processing Resources
NHB 2410.9	NASA Handbook: Automated Information Security, Volume I
NMI 2410.7A	NASA Management Instruction: Assuring the Security and Integrity of NASA Automated Information Resources
NMI 8610.22	NASA Management Instruction: National Resource Protection Program; Annex A; Consolidated Resource Listing
OMB Circular # A-130	United States Executive Office of Management and Budget, Management of Federal Information Resources Circular
ANSI/X3.159-1989	American National Standards Institute, C Programming Language Standard

ANSI/X3.9-1978	American National Standards Institute, FORTRAN Programming Language Standard
IEEE 1003.1-1988	Institute of Electrical and Electronics Engineers, Portable Operating System Interface for Computer Environments (POSIX) Standard for System Interface
IEEE 1003.2-1988	Institute of Electrical and Electronics Engineers, Portable Operating System Interface for Computer Environments (POSIX) Standard for Shell and Tools
IEEE 1003.5-1988	Institute of Electrical and Electronics Engineers, Portable Operating System Interface for Computer Environments (POSIX) Standard for Ada Language Bindings
IEEE 1003.6-1988	Institute of Electrical and Electronics Engineers, Portable Operating System Interface for Computer Environments (POSIX) Standard for Security Extension
IEEE 1003.8-1988	Institute of Electrical and Electronics Engineers, Portable Operating System Interface for Computer Environments (POSIX) Standard for Networking
IEEE 1003.9-1988	Institute of Electrical and Electronics Engineers, Portable Operating System Interface for Computer Environments (POSIX) Standard for FORTRAN Language Bindings
FIPS PUB 146-1	Federal Information Publication, Government Open System Interconnect Profile (GOSIP)
FIPS PUB 151	Federal Information Publication, POSIX: Portable Operating System Interface for Computer Environments
MIL-HDBK-217F	Military Handbook: Reliability Prediction of Electronic Equipment
MIL-HDBK-472	Military Handbook: Maintainability Prediction
MIL-STD-470A	Military Standard: Maintainability Program for Systems and Equipment, Task 104.
None	National Computer Systems Laboratory (NCSL) Bulletin, Guidance to Federal Agencies on the Use of Trusted Systems Technology

2.3 Information Documents

The following documents are referenced herein and, amplify or clarify the information presented in this document. These documents are not binding on the content of this Report.

420-03-04	Goddard Space Flight Center, EOS (Earth Observing System) Requirements, Level 1, Version 1
None	Distributed Active Archive Centers (DAAC) Strategy/Management Plan

None	Goddard Space Flight Center, Earth Observing System Mission Operations Concept
None	Goddard Space Flight Center, EOSDIS Version 0 to Version 1 Transition Plan, by Hunolt, Greg
None	Goddard Space Flight Center, Mission Operations and Data Systems Directorate: Automated Information Security (AIS) Policy

This page intentionally left blank.

3. ECS Technical and Programmatic Context

3.1 ECS Architecture

The ECS architecture provides for operational elements consisting of the EOS Operations Center (EOC), Instrument Support Terminals (IST), the Information Management System (IMS), Data Server and Ingest, System Monitoring and Control (SMC), support terminals, the Communications and System Management Segment (CSMS), and the EOSDIS Science Network (ESN). These operational entities are designed to clearly delineate functional responsibility, thereby minimizing performance risks. Ultimately, the architecture will be integrated with nine DAACs through the NASA network facilities.

Risks are associated with the EOS ground system as an extensive set of geographically distributed facilities, owned and operated by various organizations with different management philosophies and performance perspectives. Some facilities perform unique functions, while others perform similar functions using the same processes to address different scientific interests. The ECS is developed under an EOS contract through a procurement agency different than for the other EOS contracts. All of the EOS contracts are integrated at a higher level and conform to an Earth Science Data and Information System (ESDIS)-level set of requirements. Frequently, these high-level requirements are interpreted differently by the various agencies and contractors, introducing an element of risk.

To perform as an integrated, useful, and effective system, the ECS elements must interact with EOS elements developed by other contractors. Users will interface with these systems to retrieve data for analysis, to store and archive information derived from their studies, to support research programs, and to share and exchange data and ideas. The ECS programmatic risk assessment results are presented in Section 7 of this document. Section 4 defines the process used by System Integration and Planning (SI&P) to evaluate the impact of the risks on the ECS Project and the method used to mitigate these risks and ensure ECS Project success.

3.2 ECS Development Approach and Schedule

The risks associated with the ECS Project have been identified, prioritized, and categorized by user interaction, architecture, technology, evolution, systems operations, and programmatics (refer to Table 3-1).

Section 8, Risk Control and Monitoring, details the priority risks and key strategic decisions by which the risks must be resolved. The decisions are tied to a milestone or event supporting the Release Schedule.

Each risk has been individually presented to the Risk Management Panel (RMP) for program-level management discussion of the problem and the activities (modeling, prototype, studies) planned to provide sufficient information to resolve the issue without impacting cost and schedule.

Table 3-1. ECS Programmatic Risks (1 of 2)

Number	Risk Title
	User Interaction
U-1	User/Data Model Uncertainty
U-2	Earth Science (ES) Data Model Interoperability
U-3	Uncertainty of Datasets Available for ECS
U-4	Increasing Size of Standard Products
U-5	Algorithm Integration Efficiency
U-6	Interface with Advanced Spaceborne Thermal Emission and Reflection Radiometer (ASTER) Instrument Control Center (ICC)
U-7	Application Protocol Interface (API) Toolkit Maturity
U-8	Product Dependencies
	Architecture
A-1	Global Change Data and Information System (GCDIS) and User Data Information System (UserDIS) Support Approach
A-2	Resource Management with Diverse Users
A-3	Space Asset Safety
A-4	Flight Operations Segment (FOS) Distributed Scheduling
A-5	User Interaction with Archived Data
A-6	Commercial-Off-The-Shelf (COTS) Full Lifecycle Cost
A-7	Communications Service System (CSS) Overhead
	Technology
T-1	Immaturity of COTS Distributed Computing Products
T-2	Earth Science Data Language
T-3	Storage Management Interoperability Standards
T-4	COTS Hierarchical Storage Management (HSM)
T-5	Cost-Effective Storage Technology
T-6	Communication Infrastructure Performance
T-7	Database Management Systems (DBMS)
T-8	COTS Integration — Is There Enough Glue Code?
T-9	Distributed Communication Environment (DCE) Availability for Release B
T-10	Object Management Framework (OMF) Availability
T-11	CSMS Service by Platform
	Evolution
E-1	Effect of Evolution Category 3 Changes
E-2	Evolutionary Development Process
E-3	Data Storage Evolution
E-4	Multiple Versions in Operational Use Simultaneously
E-5	Multiple Spacecraft Accommodation
	System Operations
S-1	Scope of ECS Operations in DAACs
S-2	Data Distribution Automated Operations

Table 3-1. ECS Programmatic Risks (2 of 2)

Number	Risk Title
	System Operations (continued)
S-3	Command and Control Automated Operations
S-4	Quality Assurance Automated Operations
S-5	User Support Automated Operations
S-6	GFE Circuit Timeliness
S-7	Release B Production and Planning
S-8	ASTER and EOS Data and Operations System (EDOS) Late Award
	Programmatic
P-1	Software Reuse process
P-2	System Verification Environment
P-3	Compressed Development Schedule
P-4	COTS Integration Code Resources
P-5	Release-to-Release Transition
P-6	Object-Oriented Development Methodology (Systems Engineering and Software)
P-7	Operations Concept and Multi-Segment Integration

Part of the ECS Project risk mitigation strategy is the Multi-Track development process. This project management approach develops a formal track (Release), an incremental track (EP), and an Integration and Testing (I&T) activity. Each risk has been assigned a Release, or formal track, by which the risk must be resolved. Figure 3-1 reflects this association.

Risks are frequently reduced to requirements that are not standards compliant. Sometimes the technology to support the implementation does not exist. Under such circumstances, a strategy for evolving a flexible system is necessary to meet future Release requirements. This strategy is used to resolve many ECS risks. The Multi-Track strategy adjusts time to resolve an issue or defers requirements until the technology has matured.

3.3 Interaction of Risks and Project Development Activities

Within the ECS Project, each departmental organization defines a set of risks associated with the tasks to be performed. The following brief discussion identifies the risks introduced by organizational functions and operations.

3.3.1 Risks and the Requirements Process

In the ECS Project, there is a risk that the number and scope of requirements will grow. In a cost plus award fee environment, this growth could ultimately increase the work load beyond the capability of the organization to maintain the schedule within budget. Due to the evolutionary nature of the ECS, controlled requirement growth is managed through systems and Change Order process configuration control. Curtailing requirements growth to keep costs within budget is a task shared by NASA and the Hughes contractor team.

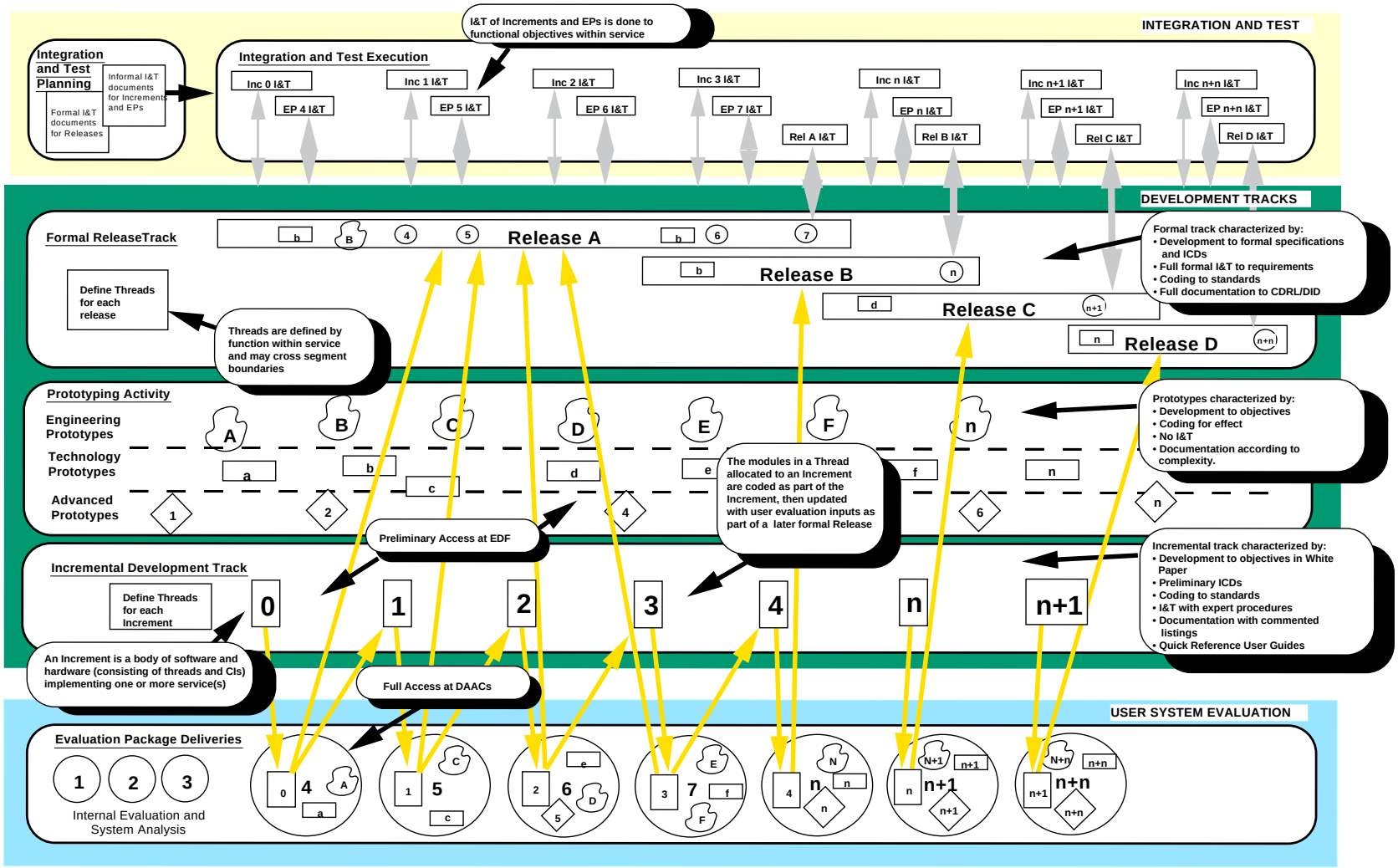

Figure 3-1. ECS Development Approach

The following steps have reduced or mitigated ECS Project requirements growth:

a. Requirements Agreement. It is important to formally agree with the customer on overall requirements as early in the project as possible. Preferably, this agreement is reached during the proposal with a well-written, detailed, customer-provided requirements specification. Alternatively, agreement is reached at the PDR. ECS was able to establish an agreement and understanding of the requirements prior to PDR despite the complexity of the flight operations, the Science Data Processing System, and the CSMS.

b. Requirements Baselining. Once an agreement has been reached, it is important to baseline the requirements immediately. The ECS requirements were formally documented in the Functional and Performance Requirements Specification, June 1994. It was equally important to ensure that all stated requirements, derived requirements, and Government-Furnished Information (GFI) be included in this baseline through the Review Item Description (RID) process. Each Release in the development lifecycle will conclude with an upgraded and expanded baseline. The team has focused on successfully attaining milestones by completing each Release in full compliance with the allocated requirements.

c. Requirements Configuration Control. Once the requirements were identified, agreed upon, and baselined, they were placed under configuration control to provide project personnel sufficient direction to continue product development, and to determine which requirements are associated with each Release.

d. Change Orders. The ECS Contract allows scope changes via the Engineering Change Process (ECP). Change Orders are cooperatively managed by NASA and the Hughes contractor team.

3.3.2 Information Engineering Practice Risks

In the past, software development has be classified into two activities: software engineering, and information engineering. Software engineering has been defined as the discipline used to specify, design, and program computer software. Software engineering emphasizes computerized process logic and encompasses software development techniques and tools, including structured analysis, design, and programming. Information engineering has been defined as the interrelated disciplines necessary to build a computerized enterprise based on data information systems. These conventional system development activities are cumbersome and have encountered a growing dissatisfaction. This growing dissatisfaction is mitigated by a new strategy which does not entirely eliminate the DBMS problems identified in the discussion of paragraph 7.11, Database Management Systems, (T-7).

The heart of the ECS design is a relatively new strategy for real-time design using an object-oriented approach. The ECS design addresses all aspects of the system development as an entity and reduces the potential for misinterpretation and redundancy. The new strategy can manage ever-increasing computer hardware capacities and capabilities and enables effective transition to high-order source code development. The object-oriented design views the hierarchical and iterative nature of the ECS systems and systems development as an opportunity to reuse software and reduce the work effort. The ECS contractor follows the practices established for an object-

oriented design. These standards are less stringent and permit the contractor the latitude necessary to evolve from design to implementation.

Assessment of the Relational Database Management System (RDBMS), Object-Oriented Database Management System (OODBMS), and Object Request Database Management System (ORDBMS) will undoubtedly reach some conclusion. The options are to convert to one standard, or to develop a translator that will convert information for communication internally between the segments and/or convert data when it is transmitted from site to site during product generation. Both options have an associated cost and impact. ECS is currently working to resolve the DBMS problem. It has been elevated to the highest level of attention, and the most capable engineers in each segment are working to resolve the impediment.

The fact that the RDBMS may not meet the ECS functional and performance requirements for spatial, temporal, and coincident search illustrates the risks of associating information engineering practices with software development and the standards and practices followed by the contractor. ECS has:

a. Trained and instructed personnel in current software development technologies.

b. Trained and instructed personnel to understand and use all standards documentation.

c. Evaluated the selected engineering practices employed to ensure that software products meet stated requirements.

d. Ensured with each Release a low-risk solution in terms of the architecture and engineering practices.

e. Evaluated COTS products to ensure compliance with all standards and practices.

3.3.3 Reducing Information Engineering Risk

The ECS information engineering approach is supposed to decompose the application into independent elements by first creating a database definition containing all of the data required by users interested in the application. The applications are then defined. An application, by definition, either puts data into or takes data out of the database. The data is converted into an action document or is used in an analysis requested by a Principal Investigator (PI). Using this approach, developers find it easy to grow applications by adding programs that perform new functions.

Typically, these types of application are implemented in an appropriate Fourth Generation Language (4GL). This does not mean that other language implementations are not used, only that the preferred way is to use a 4GL. Once the database and the initial set of applications are in place, users will apply the 4GL to query and/or grow the application by adding new programs or by performing *ad hoc* analyses. This is especially true when the fundamental purpose of the application is to provide science data to the user community. Benefits of this approach may be summarized as follows:

a. In many data and information engineering environments, data is much more stable than processes are. By first analyzing data requirements and developing an appropriate data model, a long-lasting structure can be developed to facilitate the addition or deletion of

more dynamic processes. This reduces the cost of change and increases application responsiveness.

b. Separating processes into individual, independent modules which interact only through the database reduces program design, implementation, testing, and maintenance complexity.

c. It is less difficult to grow the application using the database design concept; and it is easier to maintain congruence between the application and the changing environment by adding new programs or deleting existing processes.

d. The database facilitates change control.

Features of this risk-reduction approach offer enormous dividends. For example, application lifecycle costs are reduced. In the more traditional approach of developing tightly integrated applications, programs that interact with each other directly or through data managed by some program increase risk. In addition, information systems are: more difficult to design, because many applications interact with each other; more difficult to implement, for the same reason; more difficult to test and integrate; and much more difficult to change once they are implemented. These impediments drive lifecycle costs up.

In traditional systems development activities, these integrated applications are typically implemented using Third Generation Languages (3GL), not 4GLs. Thus, potential productivity gains are reduced. An approach which implements an information engineering application (using a 4GL) with a set of engineering practices normally applied to an integrated application (using a 3GL) often increases risk.

3.3.4 Interface Control

Interface control is often an area of high risk. The problem can be traced to the proposal phase or, in some cases, back to the pre-proposal phase. It is during these early phases that the interfaces first should be defined and outlined. In many instances, personnel simply lack sufficient knowledge about the related systems with which ECS systems must interface. Lack of interface definition contributes to unstable requirements and poses contractual problems (in scope) when the newly developed system cannot or does not interface with internal systems and subsystems, or cannot integrate with external systems and subsystems. The following solutions have been identified:

a. Define and approve baseline interfaces (both internally and externally) during the pre-release lifecycle phase. In some cases, the interfaces are well defined. In other cases, as when more than one contractor has interface responsibility and the Government assumes the role of systems integrator, the interfaces have not been defined at all.

b. Once baselined, interfaces should be placed under configuration control as early as possible.

c. The operational environment should be assessed and reviewed with the customer. All interface requirements not previously identified should be properly documented. Interface Requirements Documents (IRD) and Interface Control Documents (ICD) should establish

the physical interface. Interface Control Working Groups (ICWG) should be established if the system interfaces are significant in number, as they are for ESDIS. Failure to act promptly will increase program risk, result in customer dissatisfaction, and delay supporting data acquisition and distribution.

3.3.5 Configuration Control Board

Implementation of a high-level Configuration Control Board (CCB) is paramount to cost control. High-level implies that effective configuration control cannot be carried out at levels below that of the Project Manager. The ECS Project Manager ensures that configuration control is accomplished, and that changes impacting the ECS Project are properly controlled.

The CCB must meet regularly and frequently. Because the ECS Project is evolutionary with evolving requirements, it is recommended that the CCB meet at least once per week. During the current design phase, the CCB meets twice weekly.

As indicated, the CCB should be chaired by the ECS Project Manager. The customer's Project Manager and Contracting Officer's Technical Representative (COTR) should also attend these meetings. An open invitation has been established for this purpose, and customer attendance has been requested. The chairperson's task is time consuming, but cannot be delegated. The argument that the Project Manager has other, more important tasks cannot be accepted. These CCB meetings will resolve configuration matters and issues such as Release priority shifts, schedule changes, and resource management assignments. The CCB is the primary instrument for overall program management. Tracking change items, setting agendas, soliciting appropriate participants, and all other tasks required for CCB efficiency will require significant logistical support appropriately managed by the configuration control organization.

Change in scope creates major risks in all system development areas. A change in scope most often takes the form of a contractual Change Order, and normally requires that a mini-proposal be submitted to the customer describing how the additional work will be completed. Typically, the personnel assigned to a development task are required to respond to the Change Order. A change in scope impacts the ability of personnel to accomplish ongoing task assignments, tends to cause confusion, and creates a state of flux in the development environment. Large changes tend to be disruptive and increase program risk, regardless of the phase in which the changes occur. If possible, therefore, systems changes should be implemented within the ECP rather than outside of the change management structure.

The impact of scope changes were recognized early in the ECS Project. Such disruptive changes are inevitable in the ECS environment, but recognition of these changes allows management personnel to plan for and minimize the inherent risk and impact to cost and schedule.

3.3.6 Product Assurance

A risk-generating area for many projects is the degree to which the customer, user, and contractor cannot agree that a product is acceptable. Risk is also induced when there appears to be no incentive for the customer to accept the product, even if the product complies with the

contract, and all of the CDRLs and DIDs have been delivered correctly. The following items have been initiated to mitigate risk in this area:

a. Initiate closer coordination with the customer, especially during CDRL development. Initiate iterative informal reviews with the ECS customer's technical management personnel, the science community, the users, and the COTR to increase the probability of acceptance.

b. Assist the customer to quantify acceptance criteria by identifying the criteria in thread build test scenarios. Subjective evaluation criteria will almost always delay final acceptance.

c. Use performance data, statistical inference, min-max decision theory, etc., to quantify the subjective process.

Negotiated system use by the user community provides functional familiarity before acceptance testing. The incentive to formally accept the system is higher if the customer is allowed to operate the system prior to acceptance.

3.3.7 Cost Control and Personnel

For the ECS Contract, every dollar saved enhances risk avoidance for NASA and the Hughes contractor team. This underlying theme is stressed at the project management, staff, and technical levels of the project. It cannot be understated. Failure to contain cost will not be consistent with project goals.

This subparagraph addresses the nature of risks associated with project management and ways in which those risks can be mitigated. The material covered is based on contract price and cost control. Contract price and cost control represent areas which will require the particular attention of the Project Manager and to which a substantial amount of time will be devoted. The manner in which each of these areas is carried out will directly and indefinitely affect the ability of the program as a whole to contain cost.

3.3.7.1 Personnel Indoctrination

All personnel were indoctrinated on the nature of the ECS Contract and its impact on project development. This indoctrination began early in the contract and continues to be a theme in weekly status meetings and in the orientation and training presentation. It is imperative that all personnel be aware of the ECS Project's development approach and way of doing business. New hires are indoctrinated immediately, and current information is provided to all employees weekly.

All personnel are informed of the impact of individual job performance on project success. Individual performance is stressed by the Project Manager in quarterly performance reviews with all staff members and at weekly status meetings. Team contractors review performance and make evaluation results available to NASA and Hughes, stressing goals for the coming quarter. All ECS personnel are aware of the review cycle, in which honorable mention is given to those who excel in task performance and in meeting contract environment requirements.

ECS has demonstrated a willingness to realign and re-staff as the project evolves and contract environment requirements change. Most recently, the ECS contractors have reorganized to enhance control of the project development environment. ECS has also demonstrated a willingness to address and re-negotiate team responsibilities appropriately as requirements and technologies change. Currently, organizations unite team members with particular expertise to develop a product most effectively.

3.3.7.2 Personnel Selection

Selecting the right people in a contract environment can reduce project risk or mitigate existing threats. Selecting people with a propensity to embellish without contract re-negotiation can lead to run-away costs and major schedule slippage. Selecting people with a tendency to let the customer alter requirements without contract re-negotiation can also add cost and extend the schedule. People should be selected for all types of positions and phases in the project environment. People should not be swayed easily by out of scope tasks, but they should be customer oriented. This is especially true for the Project Manager and the segment managers in decision-making positions.

For many contracts, the contractor hires or assigns a team for the duration of the contract. Yet, in a cost plus contract, it may not be cost effective to maintain the same skill sets and labor grades for the duration. It may be more cost effective to move people in and out of the program as needed. To move people in and out of the contract as it progresses from phase to phase requires considerable forethought. Selection of appropriate personnel, therefore, is critical. The following items should be considered:

a. Moving Expenses. Moving people from one location to another is extremely expensive and adds to project cost.

b. Frequent Lay-off. As a corporation moves into a new geographic area, it is imperative that the corporation set and maintain a favorable image with the local technical population. Indiscriminately hiring and firing (off-loads) in a community will discredit the company, making it difficult to hire skilled personnel in the future.

c. Body Shops. The high cost of labor and support skills often leads contractors to hire temporary personnel to develop short-term tasks. Temporary personnel with critical office skills are currently employed by the ECS Project.

d. Temporary Duty. Frequently, personnel with high-level, specialized skills critical to project success are procured from the corporate office for short-term assignment.

Every program aspect relies on the skills, efforts, and actions of its people. The following guidelines should reduce task assignment risks:

a. Job Requirements. In the early phases of the ECS Contract, job tasking definition required great care. Specific areas of expertise were defined before recruiting people for the program. Independent assessment of required skills was tasked to executive planning. Job tasks were not defined based on available personnel. Instead, tasks were defined prior to selecting personnel with the experience, skill, and/or education to staff the project.

b. Assignments. Assignment, or job description sheets, were generated and completed before selecting the ECS staff. Understanding roles, responsibilities, and performance measurement criteria enabled outstanding results.

c. Prior Success. Personnel with proven records of accomplishment were selected to fill contracts, project management, development, design, and implementation positions. The objective was to acquire a staff of previously successful personnel. Prior success and related experience are often the primary characteristics contributing to program success.

d. Knowledge. Many positions require flexibility of skill and effort. A software system, for example, requires the integration of many skills (design, analysis, test, configuration management, etc.). An employee with broad education and experience will reduce risk by a much higher degree than an employee whose skills are very specialized.

e. Initial Staffing. Programs that begin without a complete staff begin behind schedule and assume greater risk. A program's early stages are vital to the learning and communications processes. The ECS Project was staffed from inception with qualified, committed personnel; and job description sheets were used to project future skill and personnel requirements.

f. Training. Training and familiarizing personnel with system requirements began before contract win, continued through the PDR, and are projected throughout the lifecycle. Project members are cognizant of new techniques, tools, and methods affecting project development. Training is expensive, but reduces risk in the long run.

g. Key Position Myth. ECS program management recognized that key positions do not encompass management and team leads only. Data and information systems are built by non-management personnel. In building a successful team, key positions at the working level were not minimized. The importance of one skilled and dedicated person in areas such as data modeling, prototyping, programming, database, communication, risk assessment, quality assurance, reliability, and configuration management, was not overlooked.

h. Backup. Every key position should maintain at least one qualified backup designated in writing or listed in the organizational charts.

i. Tools. For project team members to be effective and efficient, appropriate tools must be available. Computer systems and software tools to enhance engineering productivity include Requirements and Traceablity Management (RTM), Computer-Aided Software Engineering (CASE), Block-Oriented Network Simulator (BONeS), Software Through Pictures (StP), Software Through Pictures/Object Modeling Technique (StP/OMT), and ClearCASE. Without appropriate tools, the project is at higher risk from lack of system management, control, and knowledge of modeling and testing results.

j. Salary. Personnel studies indicate that if software development employees are happy with work assignments and feel that they are making valuable contributions to a project, salary is not a driving consideration. Salary does become an issue if personnel are unhappy or feel that they are not contributing. Unhappiness and low salaries can cause low morale, frustration, and lower productivity, contributing to overall project risk. The Hughes

contractor team continuously assess its position with regard to industry personnel typing and salary curves. The team competes in different environments including: engineering support to internal aerospace customers; professional services; facilities management; and systems integration to internal and external customers. The only common element is that they are all primarily Government-oriented work environments. Since it is nearly impossible to equalize salaries in each type of environment, salary levels are adjusted to meet the levels of other contractors bidding and contracting in similar environments: systems integration to systems integration, facility management to facility management, and personal services to personal services. To implement such a strategy and reduce the risk due to salary variance, individual salary structures have been implemented within each of the team's corporate divisions.

4. ECS Risk Management

4.1 ECS Risk Management Panel

4.1.1 Introduction

The RMP's purpose is to provide to project management advice and cross-disciplinary information to make risk management decisions. The RMP is a sustaining interdisciplinary panel that coordinates and measures ongoing risk management activity. The panel provides accurate current data and multi-disciplinary input to project management so that informed decisions may be made to manage project risk. Integration of risk management across technical, cost, schedule, multi-activity, and contractor dimensions is a value-added benefit to the project.

4.1.2 Risk Management Panel Members and Responsibility

Decision-making risk management authority is explicitly delegated to the Deputy Project Manager (DPM) who chairs the RMP. The panel members are the ECS Project's office managers. The primary roles and responsibilities of these panel members are detailed in Table 4-1. Their major goal is to attain interdisciplinary risk management. Therefore, these nominal responsibilities should not restrict the interaction and input of panel members. Other subcontractors (team members) participate when matters pertinent to their allocated project tasks are on the agenda.

4.1.3 Risk Management Panel Process

The RMP acts as a reviewing body at each checkpoint of the iterative risk management process defined in PI PM-1-003 (see Figure 4-1). The identified potential risks, estimates, evaluations, and resulting risks selected for management and monitoring are subject to this review. The RMP approves or redirects mitigation activities at each checkpoint in the risk management process. It is intended that management-level decision making and deliberation regarding risk management actions occur within the RMP. It is further intended that these decisions be reported to other relevant management forums, such as the Project Review, CCB, and monthly status meeting members. Issues or feedback emerging from these forums and requiring further deliberation on risk management actions are referred back to the RMP.

Each selected item in a risk management plan is defined in terms of the parameters delineated in Table 4-2; these items may be completed incrementally. This format attempts to be as quantitative as possible. This planning framework establishes the metrics monitored by the RMP. Each checkpoint in the process (see Figure 4-1) receives feedback in the form of ratification, redirection, and/or corrective action from the RMP as directed by the DPM.

Table 4-1. Risk Management Panel Membership, Roles, and Responsibilities

Member	Role	Primary Responsibilities
DPM	Chair	Decision-making authority
Systems Engineering Office Manager	Risk management planning	Implements and coordinates the risk management process, performs tradeoffs, evaluates lifecycle costs, reports status to the RMP, and updates risk status reports
Chief Systems Engineer	System integrity advocate	Integrates/evaluates proposed risk actions to ensure that system goals and objectives are achieved
Quality Office Manager	General secretary	Ensures that the risk management process is applied, independently recommends corrective and preventive actions, and monitors risk performance metrics against plans
Project Scientist	Science advocate	Evaluates science user community satisfaction impact on all risk actions
FOS Office Manager	FOS advocate	Evaluates FOS impact of all risk actions, and implements allocated part of risk actions
Science Data Processing Segment (SDPS) Office Manager	SDPS advocate	Evaluates SDPS impact of all risk actions, and implements allocated part of risk actions
CSMS Office Manager	CSMS advocate	Evaluates CSMS impact of all risk actions, and implements allocated part of risk actions
Operations and Maintenance (O&M) Office Manager	O&M advocate	Evaluates O&M impact on all risk actions, participates in lifecycle cost tradeoffs, and implements allocated part of risk actions
Independent Acceptance Test Organization Manager	System test advocate	Evaluates the testability and the Independent Verification and Validation (IV&V) interface impact of risk actions
COTS Procurement Manager	COTS technology advocate	Evaluates COTS availability and pricing impacts of risk actions
GSFC Representative	Customer	Provides GSFC's view and input on in-process risk decisions

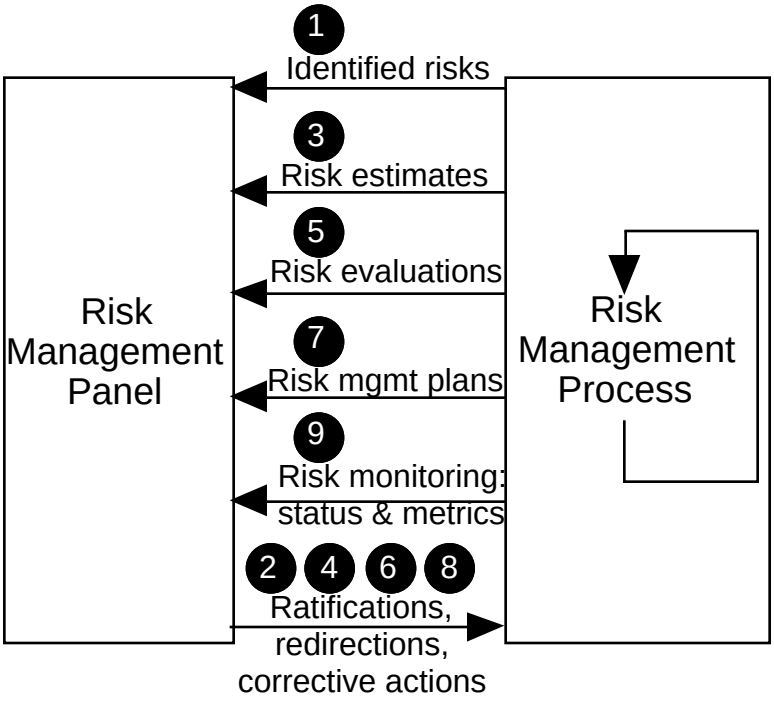

Figure 4-1. Risk Management Panel Process

Table 4-2. Risk Item Attributes

Attribute	Description
Risk Item Number	Program-unique number
Risk Item Name	Name of risk item
Description	Textual description of risk item
Potential Impact	Description of impact to program, in terms of cost, schedule, and performance, if risk comes true
Risk Factor	Numeric value based on probability and consequence of risk
Current Mitigation Plans	Specific tasks to mitigate risk (e.g., prototyping), including status of plans and responsible organization
Monitoring Thresholds	Specific values on the monitoring scale which define success or require additional action. A threshold resulting in a reduction of the risk factor to a low level is termed a success threshold. A threshold requiring additional mitigation activity is an action threshold
Scale	Measurement scale relevant to monitoring thresholds for a risk item

4.1.4. Risk Planning Quality Checklist

All risk plans should subscribe to the quality attributes delineated in Table 4-3, which can be employed as a checklist to evaluate the consistency and completeness of risk management plans presented to the RMP.

Table 4-3. Risk Planning Quality Checklist

Attribute	Quality Checklist Items
Description/Potential Impact	Is the source of the problem clearly stated? Is the impact clearly stated if the risk is not resolved? Are the activities, organizations, and system components potentially impacted stated?
Risk Factor	Is the risk factor value consistent with supporting failure probability and impact assessments?
Current Mitigation Plans	Do the mitigations listed address all of the impacts listed? Is a responsible party for each mitigation action stated? Are completion dates assigned to each mitigation action?
Monitoring Thresholds	Is an acceptable and objectively measurable success threshold specified? Are success thresholds and action thresholds traceable to mitigation actions?
Scale	Is a measurement scale specified? Is the source of the measurement data specified?

4.2 ECS Risk Management Process

4.2.1 Introduction to the Risk Process

The steps of the risk management process (see Figure 4-2) are described in the following subparagraphs. Overall coordination of this risk process is performed by the SI&P in conjunction with the Segment Offices, Quality Office, and other affected offices. At each checkpoint, the process is reviewed by the RMP as chaired by the DPM, who has authority for the team's risk decisions (including corrective actions) across cost, schedule, and technical dimensions. Project-wide risk evaluation will be performed and documented prior to each Release in the subsequent DID 210/SE3 for each IRD.

4.2.2 Risk Identification

A list of risk items is maintained by SI&P throughout the program. This list was created during the proposal and will be updated continually during the project by the risk management process. During the Phase C/D pre-proposal activities and the Phase B study, program requirements were analyzed for potential risk sources. Areas of potential risk in terms of technical, cost, and schedule impact were identified, categorized, and summarized. Additional risk sources have been identified through visits to ECS-related data centers; participation in Earth science community working groups; results from ECS team member Independent Research and Development

(IR&D), prototyping, hardware benchmarking, performance modeling and simulation, and special trade studies and analyses; review of other EOSDIS-related reference documentation; review of team member historical lessons learned databases, and RIDs generated as a result of the System Requirements Review (SRR), the System Design Review (SDR), the PDR, and the Critical Design Review (CDR). Risk items will continue to be identified in this manner for the duration of the program.

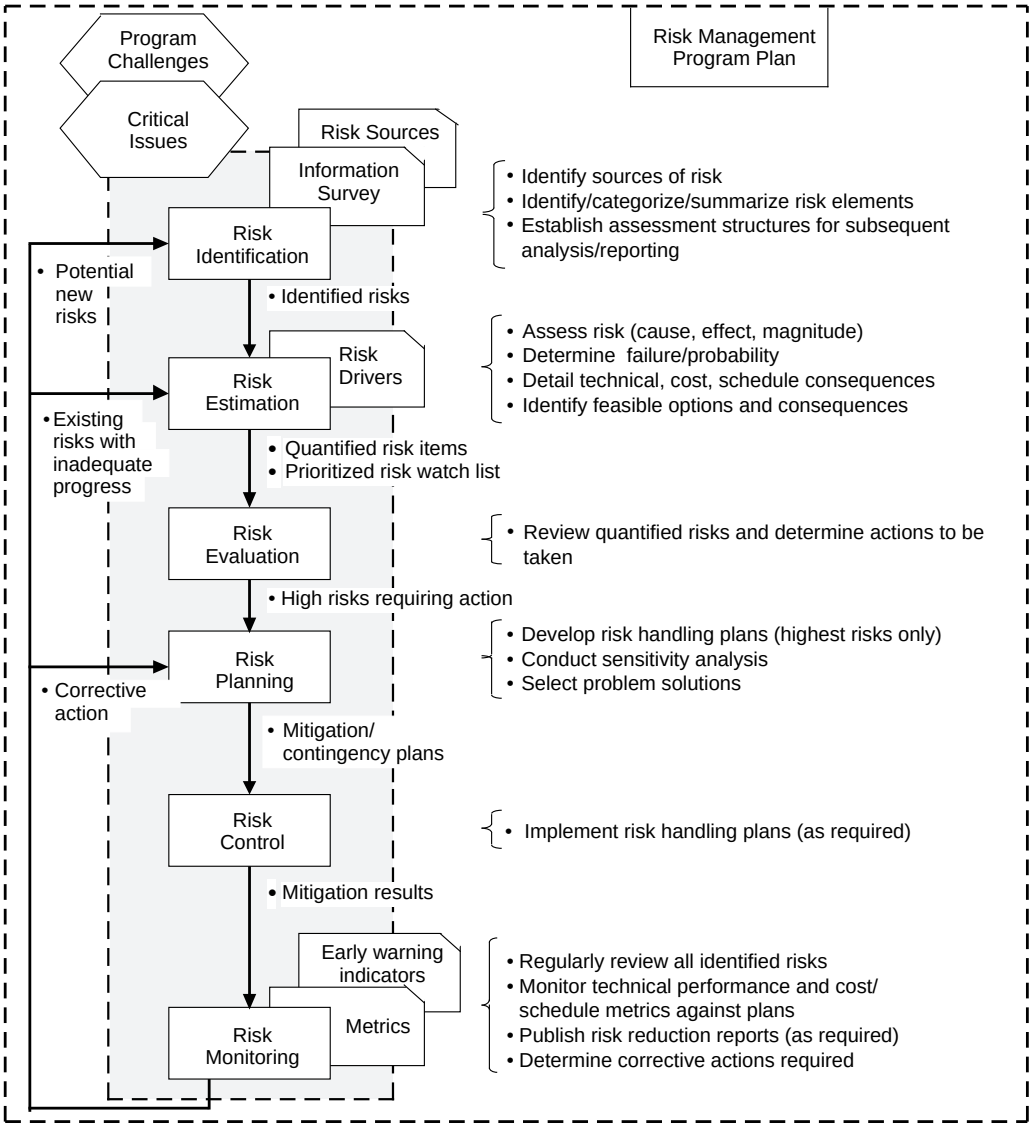

Figure 4-2. Risk Management Process

4.2.3 Risk Estimation

Detailed analyses of the identified risks and associated drivers (e.g., technology) are performed by the SI&P staff supported by other members of the segment or element development, the Project Science Office, and O&M organizations. The analyses are conducted to discover the causes, effects, and magnitude of perceived risks. They consist of evaluating all technical, cost, and schedule consequences and of determining the failure probability of deliverable hardware and software products with respect to maturity, complexity, and dependency variables. After evaluating all factors and quantifying their relative magnitude, a risk factor is calculated for each risk item. The risk factor's relative order of magnitude for a given risk area serves as a project management decision aid. It determines the necessity and urgency of devising and implementing a series of increasing scope risk-handling and risk-monitoring activities to maintain system performance within projected ECS Project cost and schedule constraints.

Risk estimation results in determining a risk factor, R_f, for each risk item. The risk factor is determined by estimating the probability of failure, P_f, and the consequence of failure, C_f. C_f is determined by technical, cost, and schedule factors (refer to Table 4-4). P_f is determined by maturity, complexity, and dependency factors (refer to Table 4-5). R_f is calculated from P_f and C_f in the following manner:

$$R_f = P_f + C_f - (P_f * C_f).$$

Several sample risks with various probability and consequence values are listed in Table 4-6. The relation of P_f and C_f to R_f for the sample values is illustrated in Figure 4-3. Values for the factors listed in Tables 4-4 and 4-5 will be provided for specific risk items by the individuals identified by the DPM. The value of the risk factor typically discussed by the RMP will be the value as calculated in Figure 4-3 multiplied by 5. The highest attainable risk factor is a 5.

Risk estimation products include quantified ECS risk items, identified project-specific causes of risk, and a prioritized risk watch list encapsulating for each risk area things such as indicators of the start of a problem and candidate risk mitigation techniques. The risk list shall contain attributes for each risk item as detailed in Table 4-2. Information about an attribute shall include the information source(s).

4.2.4 Risk Evaluation

Feasible risk mitigation options are developed for high-risk items. The most feasible and effective options will be developed further as part of the risk planning stage. The options should contain specific action plans, including implementation criteria (i.e., success and action thresholds). The plans may be contingency plans in case of failure, mitigation plans to proactively reduce risk exposure, or both contingency and mitigation plans. Values of risk probability and consequences shall be considered. For sample risk #2 (refer to Table 4-6), the mitigation plans would attempt to reduce risk consequence. For sample risk #3 (refer to Table 4-6), the mitigation plans would attempt to reduce risk probability. The type of risk shall be considered when developing the plans. For a risk caused by an external source, for example, the plans would attempt to reduce the risk item's consequence, as the probability may be unaffected by project action. For project-internal risks, the plans may attempt to reduce project-controlled risk probability, as reducing risk consequence may lessen the project's ability to achieve its goals.

Table 4-4. Consequence of Failure Calculation

Magnitude of C_f	Technical Factor (C_t)	Cost Factor (C_c)	Schedule Factor (C_s)
0.1 (low)	Minimal or no consequences, unimportant	Budget estimates not exceeded, some transfer of money	Negligible impact on program, slight development schedule change compensated for by available schedule slack
0.3 (minor)	Small reduction in technical performance	Cost estimates exceed budget by 1 to 5 percent	Minor slip in schedule (less than 1 month). Some adjustment in milestones required
0.5 (moderate)	Some reduction in technical performance	Cost estimates increased by 5 to 20 percent	Small slip in schedule
0.7 (significant)	Significant degradation in technical performance	Cost estimates increased by 20 to 50 percent	Development schedule slip exceeding 3 months
0.9 (high)	Technical goals cannot be achieved	Cost estimates increased in excess of 50 percent	Large schedule slip affecting segment or system milestones

$C_f = (C_t + C_c - C_s)/3$

Where C_t = consequence of failure due to technical factors

C_c = consequence of failure due to changes in cost

C_s = consequence of failure due to changes in schedule

Table 4-5. Probability of Failure Calculation

Magnitude of P_f	Maturity Factor (P_m)	Complexity Factor (P_c)	Dependency Factor (P_d)
0.1 (low)	Existing	Simple design	Independent of existing system, facility, or associated contractor
0.3 (minor)	Minor redesign	Minor increase in complexity	Schedule dependent on existing system, facility, or associated contractor
0.5 (moderate)	Major change feasible	Moderate increase	Performance dependent on existing system performance, facility, or associated contractor
0.7 (significant)	Technology available, complex design. New software, similar to existing software	Significant increase	Schedule dependent on new system schedule, facility, or associated contractor
0.9 (high)	State of the art, some research complete	Extremely complex	Performance dependent on new system schedule, facility, or associated contractor

$P_f = (P_m + P_c - P_d)/3$

Where P_m = probability of failure due to degree of design maturity

P_c = probability of failure due to degree of design complexity

P_d = probability of failure due to dependency on other items

Table 4-6. Sample Risk Items

	Risk Item	Rf *5	Rf	Cf	Pf
1	Low Probability, Low Consequence	1.0	0.19	0.10	0.10
2	Low Probability, High Consequence	3.7	0.73	0.70	0.10
3	High Probability, Low Consequence	3.7	0.73	0.10	0.70
4	High Probability, High Consequence	4.6	0.91	0.70	0.70

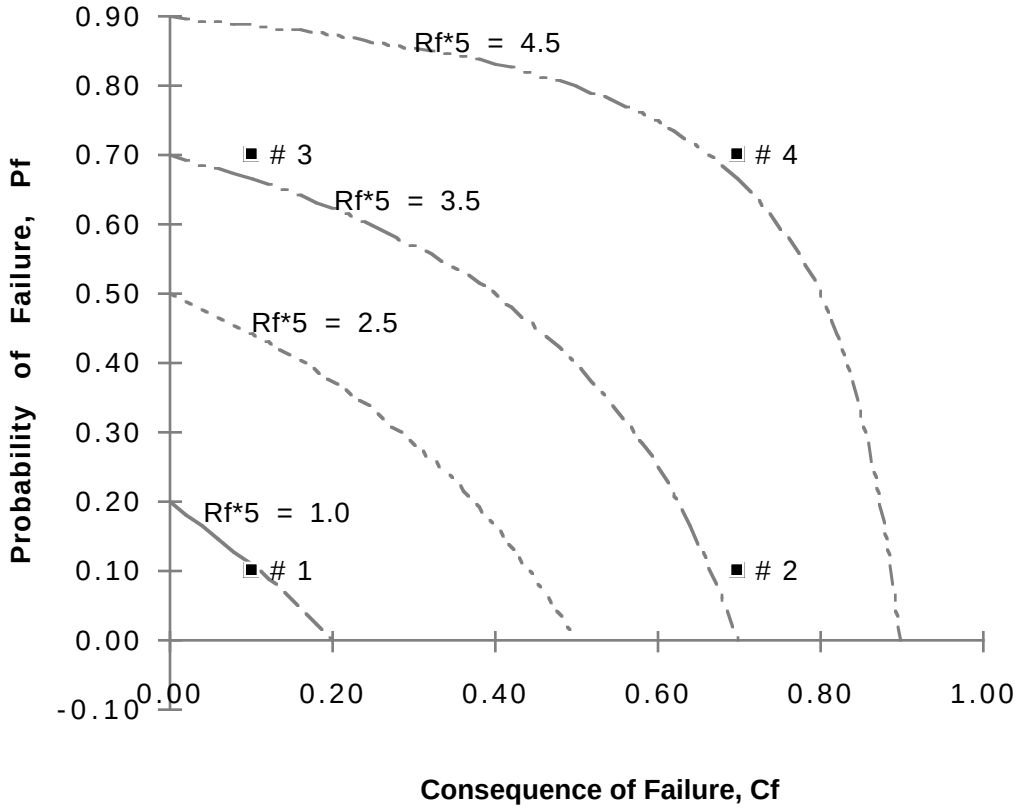

Figure 4-3. Sample Risk Items

4.2.5 Risk Planning

Much of the project organization, led by SI&P participants, is devising integrated risk mitigation plans. Alternative strategies and processes are developed, reviewed by project management, and refined. Finally, the appropriate mitigation approach is selected. Examples of mitigation and contingency plans include alternate vendor or product source selection, critical component prototyping, subcontractor performance and cost incentives, extensive development testing and EP assessment, and model or simulation development to predict performance. A detailed examination of each Work Breakdown Structure (WBS) category ascertains areas of greatest risk sensitivity. Related decision-support analyses, under project controls staff administration, help ECS project management to determine the preferred course of action. These analyses include: summarizing the technical, cost, and schedule implementation impacts for each alternative considered; projecting the overall program cost and schedule if no risk reduction action is taken; identifying the organization and personnel responsible to manage the risk; defining a risk mitigation or abatement plan with measurable schedule, cost, and technical metrics and key decision points; specifying criteria for closure of the specific risk activities; and outlining recommended backup or contingency plans.

4.2.6 Risk Control

This function is accomplished through execution of detailed mitigation plans developed in conjunction with the risk planning function.

4.2.7 Risk Monitoring

Each ECS Project functional organization manager is responsible to periodically reassess identified risk items and to identify potential new ones. Tracking the status of open and potential risk areas is an SI&P function. Technical, cost, and schedule performance of implemented risk mitigation plans are qualitatively assessed at each weekly internal project management review to ensure that risk areas, with appropriate resource priorities, are properly emphasized. Throughout the program, NASA personnel will be apprised of each risk area through monthly progress reviews, major technical reviews, monthly progress reports, the tradeoff studies analytical data report, the security analysis report, and this document.

Beginning with the in-depth estimates in the Phase C/D Cost Proposal, tools such as the Lifecycle Cost model and Performance Measurement System have been used to quickly develop cost projections assessing the downstream cost and schedule results of risk mitigation decisions. Additional metrics and parameters peculiar to the risk control process will be identified and monitored. ECS-related early warning indicators (trends versus time) include requirements and interface volatility, To Be Determined (TBD)/To Be Resolved (TBR) convergence rate, volume and content of NASA and user feedback, critical path milestone status, development and integration schedules assessment, performance requirements satisfaction, actual verses projected use of COTS hardware and software, applications of legacy and heritage software, modeling and simulation results, and fidelity of hardware technology and cost projections to actual industry trends.

This page intentionally left blank.

5. Major Risk Mitigation Activities

5.1 Introduction to ECS Risk Mitigation

Moderate, up-front investments in risk management can reduce long-term costs. Developing and integrating a data collection and information distribution system is like any other human effort: the better the environment to fulfill the mission, the greater the likelihood of attaining the objective in the planned manner. In the case of ECS systems development and integration, the environment created has emphasized the plan's high-risk points. General areas that seem to represent the greatest risk and for which the Hughes contractor team can reduce ECS Project risk through modest investments include the following three items:

a. Reach closure on prototyping application modules early to continue development activities.

b. Appraise system software performance through the Early Release Plan as subsystems are developed; encourage the customer and user to accept the software; and meet performance standards on a timely basis. This way, the ECS team, customer, and user do not have to wait extended periods of time to rate system performance.

c. During early project development, ensure that the entire project team, the customer, and the user understand the project plan and engineering practices to be used to develop the software and the system development concepts. If everyone follows the plan, the system can be built and delivered for the contracted funds with minimal risk.

Paragraph 5.2 discusses specific areas implementing innovative concepts.

5.2 Prototypes and Studies

Prototyping is the ideal way to develop the look and feel of an application or data collection and distribution system. By definition, a prototype is an engineering model of the proposed system. Several types of prototype are commonly used to develop data processing, communications, and storage systems. The following types are the most common:

a. Simulation. A special-purpose program is used to imitate the look and feel of the proposed system. When developing a simulation, the user can see what the screens will look like and be guided through a simple scenario. The user cannot use the prototype to perform useful work, but the prototype does provide useful feedback information.

b. Working Prototype. A working version of the system is built, typically using a 4GL or some other tool affording the developer very high productivity. Some people mistakenly regard the process of using a high-productivity language to prepare a prototype as rapid prototyping. Working prototypes are the most common type. This method of modeling enables potential users to select the best look and feel to acquire the necessary research data. By accessing and operating the data and information system, users can actually experience its performance characteristics.

c. First Generation System. A very common form of prototype is a first generation system. If the user has not experienced the look and feel of a system prior to its first implementation, the user probably will not find it acceptable, and will request system modification.

5.2.1 Nature of Prototyping

A major source of ECS risk is in selecting a design and development practice incompatible with the project. Prototypes afford a means to more fully understand the functionality of a system or subsystem and to minimize the risk of selecting the wrong design to fulfill a group of requirements. The prototype defines the difference between the customer's concept of the system as defined in the requirements document and the contractor's interpretation.

By definition, prototyping is limited to the requirements phase of a lifecycle. The results represent a working view of the finished system in terms of user interface and requirements. An EP, on the other hand, is the incremental build of the final system based on design maturity. An EP is an expanded version of prototyping used to provide the user community an opportunity to experience and evaluate the contractor's interpretation of the requirements. Subsequent sections of this document elaborate this discussion of EPs.

A major risk is that the project team will not understand the distinction between prototyping and EPs and will proceed with the design under a prototyping concept; when, in fact, an incremental development of the system, under tight configuration management control, is required. For ECS, the potential for misunderstanding has been minimized by assigning senior staff engineers to participate in EP activities. Once a design concept has been prototyped and integrated into an EP, the package is placed on the network for evaluation and comment by the science user community.

The ECS Contract approach requires extensive interaction with the user [PI/Team Leaders (TL)] during the initial development and Release versions. The risk mitigator is able to interactively modify the system design to meet user expectations. The risk lies in not recognizing when prototyping is complete and when the EPs should be integrated into a Release. The distinction is the point at which the EP development is placed under configuration control.

Succinctly, the risk is in not knowing when to identify a sign-off baseline from which to build the Release. This potential risk stems from a lack of experience in dealing with a diverse community offering extensive user interaction with and participation in the development process. The project team must continually progress toward a mature Release baseline for user sign-off. Digression must be avoided. Users participating in the development will significantly influence the COTR, who has sign-off authority for the established and approved Release baseline. ECS plans to manage this risk by identifying user-suggested modifications in one Release and integrating the modifications into the next Release through the EP process.

Prototyping and Release integration require a different lifecycle development methodology than the traditional waterfall serial approach to systems development found in MIL-STDs 490 and 2167. A way to clearly identify prototype requirements allocation and the flow of the proven concept into the Release is required. For ECS, this is accomplished by using RTM to trace the requirement to the Contract Item (CI) and identify the CI's association with a prototype or Release.

5.2.2 Prototyping and Risk Reduction

One risk to the ECS Project is that a clear distinction between prototyping and the purpose of the EP was not made to the user community. To minimize misunderstanding, considerable effort has been expended during various reviews to explain the relationship between prototyping and EPs. Additionally, confusion over current prototyping and older rapid development methodologies exists. Several plans clearly define the movement of the ECS development from prototype, to EP, to Release; yet the functional transition to an operational system is still unclear to the user community.

In the traditional sense, prototyping is limited to the requirements phase of the product lifecycle. The results of this approach represent a working view of the finished system in terms of user interface and functionality. Rapid development, on the other hand, incrementally builds the final system based on an immature design. Developers usually talk prototyping, while the user community understands rapid development. The developer's intention is to move from the prototype to an EP for eventual Release and systems integration.

The current approach supports extensive communication with the user community during development, and interactive modification of the system design to accommodate user requirements and expectations. The risks are in not knowing what changes support the user community's needs and potential paradigm changes. The assumption is that the user will be innovative, and will need to perform functions not supported by an ECS capability. Hopefully, the user community will discover these deficiencies while evaluating the EP. The user community must inform the developer of these needs early in the evaluation to allow the developer sufficient time to implement the requested changes. A sign-off baseline, or Release, will be identified when the user community's needs are satisfied. At this point, new technologies will be assessed. New technologies will be incorporated to more completely satisfy users and improve system performance.

5.2.3 Prototyping Risk in Tool Selection

CASE uses computers for software development and maintenance. ECS uses CASE to develop prototypes, and therein lies the risk of tool selection. Tool selection represents an inherent prototyping risk. The risk is obvious: selection may impact cost, schedule, and product design and development significantly. Software tool selection implies two broad categories: programming in the larger sense, and programming in the diminutive. Programming in the larger sense is the area of greatest risk because it involves coordinating the software to be used in the project's prototyping effort. Managing multiple versions of software, avoiding simultaneous module updates by two or more programmers, maintaining multiple system versions, and scheduling interdependent software development subprojects evoke particular concern. When tools are used by individual programmers (programming in the lesser sense), the concern is with managing compilation dependencies of program design and prototype tools, symbolic debuggers, and syntax-directed program editors.

At present, CASE refers to tools for the entire software lifecycle, including specification, design, development, maintenance, and support activities (such as prototyping and modeling). CASE tools have been classified into several broad categories: front-end; back-end; maintenance and

support software; and frameworks, or general categories describing function. In prototyping, the interest lies primarily with the back-end tools. Based on traditional programming languages and tools, there are two quite different approaches to CASE, particularly for back-end tools. These approaches are distinguished by their use of higher-level languages and packages or expert systems. Without going into unnecessary detail, using higher-level languages and packages in prototyping creates risk. ECS has emphasized the use and development of user interfaces in window systems. Large application programming productivity gains have been accomplished by focusing on one prototyped application area. Many commercial products have emphasized specific applications. For example, there are many 4GLs, forms packages, and database design tools oriented to the large market for business database applications on character terminals. Only recently have software suppliers turned to the applications ECS needs.

ECS is reported to be an object-oriented design. Product integration and prototyping software management are extremely complex. The following concerns point to a higher level of program and prototyping risk (in the tool and in CASE selection), requiring intense coordination and management:

a. Selecting tools and COTS products using lower generation languages.

b. Selecting a 3GL to meet the fourth generation development requirement.

c. Selecting a 4GL instead of an object-oriented language.

d. Selecting a combination of software languages to develop the segment prototypes (i.e., combining C and object-oriented languages).

The recommended risk mitigation language selection supports an object-oriented design. An object-oriented language should be used to prototype and incrementally develop the design, even though a 3GL (C) is the target production language.

Highly interactive fourth generation (object-oriented) development tools should be used to develop a minimum set of code to obtain maximum coverage. This reduces potential data integration across tools, promotes data collection, processing, and information distribution reuse, and promotes systems prototyping and design across EPs and Releases.

Tools should be chosen to support the deliverables under a fourth generation (object-oriented) development process, not on the basis of individual features or operating platform characteristics. Systems based on object-oriented data models originated with an object-oriented programming paradigm. The object-oriented programming paradigms considered for this project included Simula, Smalltalk, and most recently, C++. The object-oriented programming paradigm subsumes the concept of abstract data types in programming languages. Abstract data type declarations explicitly define public and private portions of a data structure or an object. Abstract data types in object-oriented languages, called classes, encapsulate private data portions of the object with public procedures, called methods. Encapsulation is used to simplify program construction and maintenance through modularization. As long as the public interface definitions are not changed, an object may be defined as a black box that can be constructed and modified independently of the rest of the system. This software development approach leads to reuse, minimization of maintenance, development schedule compression, and risk reduction.

5.2.4 Reducing Prototyping Risk

Several risks associated with prototyping have been discussed. Two common risk-associated problems remain: uniting the users and prototype developers in a productive working environment, and bringing the prototype effort to a close.

The ECS Project has selected an interactive process to evaluate the collective prototype results and to mitigate risk. Typically, the user cannot evaluate prototype results until the capabilities are assembled in an EP. The EP unites the users and the developers' prototype products in a productive working environment.

The program provides a Science and Technology Laboratory (STL), a room designed specifically to increase prototype development productivity. A team of users and prototype developers use the room for brief, intense prototyping sessions. The room is located near the NASA facility, enabling better communication. The room contains workstations selected to meet ECS prototyping and developmental requirements.

The closure process for prototype results occurs in two phases: initial assessment of the prototype results, and finalization and acceptance of the user EP assessment comments as changes to the prototype. It is difficult for the prototyping effort to achieve closure. The contractor and customer must find some incentive to close the prototyping effort. Without this incentive, time and resources will be wasted without achieving the desired results.

ECS, therefore, has incorporated a prototyping capability into the project facility. Construction required only modest capital. Items considered for the prototyping center included the build out costs for a laboratory, 6 workstations, 3 overhead projectors, workstation projectors for each overhead, white boards, a conference table and chairs, a communications interface to customer mainframes and databases, appropriate software, appropriate servers, and telephone services. The ECS team believes that the facility will enhance prototype development and improve communications with the user community, while reducing prototyping risks.

5.3 System Modeling

For ECS, modeling is used to evaluate various aspects of system performance. The risk associated with modeling is that the data is only as good as the assumptions made, the data used in the model, and the level of confidence in the output.

5.3.1 Nature of Modeling

Models are abstracts built to understand a problem before implementing a solution. All abstracts are subsets of reality selected for a particular purpose. For ECS, modeling is used as a performance assessment to determine alternative designs and the parts of the system to be modeled. In essence, a model will locate a system's performance-sensitive parts.

Models are typically validated as representative of systems or subsystems. Validation may be accomplished by evaluating assumptions, input parameter values and distribution, and output conclusions. Techniques for assessing the representative model include expert intuition, comparison with known real systems, and comparison with theoretical models under simplified conditions.

5.3.2 Modeling During Development

The static model presents the unchanging, structural data aspects of a system or subsystem. The dynamic model represents the temporal, controlled behavioral aspects of a system or subsystem.

Many critical decisions are made when designing a model. These decisions are related to the level of detail and the parts of the system to be modeled. Few firm modeling rules exist. Ideally, start with a simplified model to which detail can be added. Emphasize the parts of the model most relevant to the desired result or problem solution. A common mistake in modeling is to include excessive detail. Excessive detail generally takes too long to develop and execute. Often, insufficient information is available to warrant a detailed model. Excessive information tends to distort and cloud issue resolution.

5.3.2.1 Sensitivity Studies

Modeling risks are associated with identifying a model's sensitivity, or its capacity to respond to input parameter changes. Thus, if assumptions concerning the input parameter values and distribution [as in the Data Flow Diagram (DFD)] are in error, a small change in the input data may result in a greatly exaggerated output or result.

The basic procedure for developing a model is to determine what capabilities currently exist, remove nonessentials, add any new functions specified by requirement or by the user, and determine exactly how to implement the new design. This process occurs as a gradual transformation from the static model to the dynamic and improved dynamic models.

Modeling the logical model, or showing the incarnation of the proposed system has been suggested. The current logical model eliminates all custodial functions (that is, everything nonessential), and partitions the proposed system to better enable understanding. The following steps are suggested to build the logical model or a desired part of the model derived from partitioning:

a. Build one large DFD by connecting the diagrams two levels below the overview.

b. Remove synchronization data stores and custodial activities, such as formats and writes.

c. Restructure the database using data modeling techniques.

d. Modify the DFDs to reflect changes in the database.

e. Partition the working diagram into fragments; and use these fragments to create a set of formal DFDs, including an overview and lower-level diagrams.

The new logical model shows the essence of the new system or partition under study. New user knowledge and requirements may be incorporated by recreating or building new lower-level DFDs or by modifying existing DFDs. In modifying the overview diagram, the data structure, or in the case of an object-oriented design, the context diagrams, the data dictionary must match the changes incorporated into the DFDs. Once this has been accomplished, an output data analysis will reflect highly sensitive or insensitive design areas.

5.3.2.2 Processing Stability

The model's stability is essential. Stability is verified by validating that the model accomplishes what it should. Some techniques for verification are to:

a. Individually test sensitive parts of the model.

b. Build error checking into the model.

c. Perform a structured walk through.

d. Run simplified scenarios.

e. Trace the model's execution.

f. Assess the algorithm using an interactive debugger.

g. Analyze graphical displays of simulation variables or entity flows.

h. Perform reality checks or assessments.

5.3.3 Modeling Risk in Tool Selection

The risk associated with modeling tool selection is often mitigated during the process of choosing the modeling tool. A study, for example, will assess a tool's purpose. By evaluating the capabilities of various tools on the market, a study may recommend the tool most appropriate for a task. Appropriate CASE tools were selected for ECS to mitigate modeling risk. Modeling tools offer applications capability proven in a modeling framework.

The tool currently used by ECS to model push processing requirements and processing interdependencies is the BONeS DESIGNER™ Version 2.5. Most often, the analyst prescribes the modeling tool to be used based on experience with the tool or an assessment of the tool's capabilities. The modeling tool's overall capabilities are in and of themselves risk mitigators. BONeS provides an interactive graphical framework for modeling and simulating communications networks, distributed processing systems, and other event-driven systems. The tool's capabilities include modeling a system architecture with shared resources, executing an event-driven simulation, computing and displaying performance measures, performing design iterations and tradeoffs, and documenting and storing design hierarchies.

Other CASE products excel at creating and maintaining graphics, including data models, through symbol manipulation. For example, as a data modeling tool, CASE interacts with the data dictionary. While working at a data modeling screen, the analyst can access data or pull up a data dictionary screen to check or enter the definition for an entity or relation. Through the data dictionary, entities on the data model are linked to DFD data stores.

5.3.4 Risk Reduction Through Modeling

Modeling risk reduction is accomplished by understanding system performance and identifying areas of sensitivity. Modeling enables system understanding and identifies deficiencies and potential areas for design improvement. These areas are typically requirements changes, concept modifications, or reentry of tradeoff or trade studies.

5.4 System Evolvability Tests

ECS has planned to evolve the system as new products and capabilities evolve and mature in the market place. The prototyping and modeling methods previously discussed are part of the planned process to evolve ECS over its 10-year lifecycle.

5.4.1 Nature of Evolutionary Packaging

Modeling will validate the performance of new technology prior to system integration. Modeling features will consist of the processes described in paragraph 5.3. These include generating a technology abstract and assessing its performance by introducing real data. This assessment will identify sensitivities and provide additional information, such as bandwidth increases or decreases, processing requirements, storage requirements, and interdependencies between DAACs.

5.4.2 Risk Reduction Through Evolutionary Packaging

5.5 Data Modeling

A simple system requires only a data dictionary to recognize the relationships among the data. In a more complex system, a data dictionary alone cannot reflect these relationships adequately. This is especially true of a system with complex data of different types and connections. For such cases, we need a graphic model, ideally satisfying the following criteria:

a. It should be unique with respect to the specification tools, such as the data dictionary or set of DFDs.

b. It should model logical data, independent of the physical implementation of data storage and retrieval.

c. It should communicate with the database designer and administrator.

d. It should define the data schema precisely.

e. It should convert easily into a physical system implementation.

5.6 Data Migration

ECS data migration activities and plans are outlined in the ESDIS Project Version 0 - Version 1 Transition Plan. This plan establishes a framework for each DAAC's individual transition plan after the Release A design. The subject document identifies data and metadata migration operations to be accomplished after delivery of ECS data catalogue and storage elements to each DAAC. Refer to the DAAC Strategy/Management Plan, August 1994, for details of the data set acquisition and ingest. These plans describe future activities including the data transition from DAAC heritage to new-line DAAC systems.

Data migration involves data transition and conversion from Version 0 to Version 1 and bringing the Version 1 system to operational status. The risk associated with data migration and conversion is the discontinuity of services. Several groups have been established to help the ECS

Project and DAACs to resolve issues during data migration. The primary purpose of the groups is to mitigate the risk associated with the data migration from Version 0 to Version 1.

The working groups include representatives from NASA (ECS Project personnel), the DAACs, the contractors (ECS Project personnel), and the science community. The groups are meant to function as follows:

a. Data Migration Working Group. This group will resolve all technical issues related to the data migration process.

b. The Software Operations Focus Team (SOFT) Science Subpanel. This panel will address all science prioritization issues related to data migration.

c. DAAC Managers. This body will address all management issues related to data migration.

d. DAAC Users Working Group. This group will support risk mitigation by identifying issues and suggesting alternatives to resolve problem areas.

The parallel operations of Version 0 and Version 1 are specified as element interoperability throughout the transition period. The transition is to occur in stages beginning with Release 1. Release 1 will be a one-site operational prototype of the ECS IMS, Data Archive and Distribution System (DADS), and Product Generation System (PGS) I&T capability. Release 2 will provide IMS capability at all DAACs and a DADS functionality at some sites. All DAACs will be fully transitioned and operational with the delivery of Release 3.

The planned method of conversion for all primary copies of data held by the DAACs within the ECS is to provide a working copy to the user and to make available the tools necessary for conversion. Ultimately, all data must be translated; however, this activity is still in the planning stage. Non-NASA or external holdings will be managed in a similar manner. The Hughes contractor team's transition and migration activities include:

a. Evaluation of the Version 0 system.

b. Incorporation of Version 0 into Version 1.

c. Conversion software development.

d. Data and metadata conversion and migration.

e. Science algorithm integration.

f. Facility and site requirements development.

The risks in these activities are in conversion software development, data and metadata conversion, and integration of the investigator-provided science software. There are two conversion software development risks. The first risk is the actual software conversion and translation. The second risk is that the ECS does not manage the entire DAAC integration. The task must be performed as outlined in the Project-DAAC working agreement. Data and metadata conversion risk depends on the delivery of other ECS capabilities and the volume of data to be migrated. The risk in integrating the investigator-provided science software is the dependency on the scientist to provide the science software and algorithms as finished products. Software

revisions are frequently generated as a result of operational test and evaluation. These revisions tend to impact schedule and delay operational readiness. At this stage of development, awareness of potential risks may be recognized as a step toward mitigation.

5.7 Interface Management

ECS interface management is the responsibility of the ECS Interface Engineer. Interface management responsibilities include coordination, development, and integration of the ECS IRDs and ICDs. IRD and ICD management risks originate in the higher-level ESDIS document, the Memorandum of Understanding (MOU). This document is subject to change at the ESDIS level with serious impact to the ECS. MOUs are generated by NASA headquarters through negotiation with corresponding top-level organizations. MOUs address interfaces between NASA and the International Partners (IP) contributing to NASA's Mission to Planet Earth, and between NASA and other Government agencies.

MOUs are reflected in ESDIS Level-2 requirements and in corresponding Inter-Project Agreements (IPA) or Project Implementation Plans (PIP). IPAs and PIPs are ESDIS-level documents. They address essentially the same material; but IPAs address non-ESDIS NASA programs, while PIPs address non-NASA projects. The agreements in either document type trace upward to the corresponding MOUs and downward to the corresponding ESDIS Level-2 requirements and IRDs. The potential for a difference in requirements interpretation is considerable. Close coordination is required to ensure that interpretations are identical in the respective projects.

In addition to IPAs and PIPs, Project Data Management Plans (PDMP) are generated by each flight project providing data to the ECS. The ESDIS Project supports development of these documents by providing PDMP guidelines to other projects, ensuring project access to the documentation necessary to produce the PDMP, and reviewing the completed PDMP. Furthermore, the PDMPs are used by the flight project to develop each IRD.

Each mission specifies in its Detailed Mission Requirements (DMR) the requirements for NASA institutional support. Specifically, these documents may (and frequently do) affect the interface between NASA institutional systems and the ECS Project. The ECS Project mitigates requirement interpretation risks by closely monitoring the IPAs and PIPs for which the ESDIS Program is responsible, and by monitoring the PDMP and DMR controlled by the relevant flight project.

5.8 Project Software Development Activities

The ECS Project has adopted an object-oriented approach to design the ECS segments. The general disparity in possible definitions of the term object-oriented warrants a short discussion.

5.8.1 Development Environment

Introduction of object-oriented concepts into the ECS development environment was one of the many management decisions supporting project-level risk mitigation. In the development environment, the term object-oriented means different things to different disciplines. In the

context of ECS risk, the term will be defined operationally. An Object Data Management System (ODMS) is a DBMS geared to satisfy the needs of computer-aided design, software engineering, and other new ECS applications.

In the development environment, the applications most often cited are software engineering, mechanical and electrical engineering, and documentation. Many of these applications have similar data manipulation requirements. Regardless of the nature of the data, the principles are identical and use computers to create the programs. ECS software engineering programs are designed in an object-oriented language to provide object flexibility and program or file reuse. The object-oriented approach provides a flexible design to evolve the ECS, and minimizes long-term program maintenance and support.

5.8.2 Modeling Activities Versus Schedule

In September of 1994, Pugh-Roberts completed the ECS Unplanned Events and Design Uncertainty (risk) assessment. The results were presented to ECS project management in the RMP meeting. The activities identified as risks to the project are presented in a synopsis in this document. The assessment consists of a model-based analysis of the following simulation sequences:

a. Run # 1. As Bid Baseline (November 1992).
b. Run # 2. Award Baseline (April 1993).
c. Run # 3. Change Order 1, Imposed.
d. Run # 4. Change Order 1 and SRR Imposed (September 1993).
e. Run # 5. Multi-Track Development Adopted.
f. Run # 6. Future Direct Impacts (Sensitivity Analysis).

ECS Project changes directly and significantly impact the program. The changes are not a part of the program's originally planned work process or part of the contracted scope of work; and unplanned events generate risk. These events were initiated by NASA, the user community, or ECS management. The impacts and immediate consequences of the unplanned events are identified as follows:

a. Scope Growth. Change in technical work scope attributed to unplanned events.
b. Work Obsolescence. Work that is effectively rejected and requires re-work to meet the schedule.
c. Added Hours. Work hours from additional analysis, meetings, design studies, and indecisiveness.
d. Design Impact. Design information made unreliable, uncertain, or unusable for some period of time.

All events impact the schedule and are reflected in the Pugh-Roberts presentation. The unplanned events and uncertainties, or risks, are identified as processing and storage growth, Common Object Request Broker Architecture (CORBA) interface transparency, architectural extension for data transparency, distributed query processing, schema framework integration or federation for

user-defined methods, SMC re-engineering, PGS toolkit interface code development, CSMS incremental development, use of an object-oriented development paradigm, and COTS procurement and integration.

Key unplanned events and uncertainties are addressed individually in the Pugh-Roberts presentation. The risks identified in the report are addressed by specific description, valuation, and risk mitigation activities. All risks are prioritized, and specific risk mitigation activities are addressed in subsequent sections of this document.

5.9 Technology Assessment

Technology assessment is a process by which evaluation of equipment or software may establish a product's compliance with a stated capability or set of requirements. The process is used in the ECS environment to determine a product's compliance with performance, functional, interface, and standards requirements. Assessment of the product's performance capabilities may be accomplished on paper or through hands-on testing.

Product operation provides technical information and/or a hands-on evaluation of equipment or software. The process predicts the potential direction of future technology, its cost, availability, and performance. The assessment may determine a technology's compliance with established ECS standards.

5.9.1 Nature of Technology Assessment

Technology assessments are performed to mitigate a technical risk, support a segment or science need, lower cost, improve performance, or meet evolutionary requirements. Drivers for an ECS technology assessment include:

a. Cost or Schedule. The potential to reduce cost and meet a difficult schedule may generate sufficient interest at the program level to motivate an assessment. By accurately estimating future pricing and using this information to procure products at a time when maximum utility is realized, a significant cost savings will be generated.

b. Requirements. All requirement levels, including evolutionary requirements, have the potential to drive an assessment. Science or segment requirements often drive an assessment of a new and/or evolutionary product. Frequently, new technology will satisfy multiple requirements or offer greater functionality and performance at or below predicted cost.

c. Improved Capacity. Improving the performance of workstations, routers, servers, etc. may improve capacity.

d. Evolution. Technology assessments support evolution by indicating which products will be standards compliant in the future. To optimize cost and minimize impact, developers must know and understand the direction of future advances, their availability, and release dates.

5.9.2 Risk Reduction Through Technology Assessment

Technology assessment is an integral part of ECS technology risk mitigation. Standards mitigate risk and help to determine the direction in which a technology will evolve. Standards guide a technology's evolution by identifying its future capabilities, and predict the nature of the future state of the art.

The assessment process identifies potential software and hardware systems problems by verifying that these products conform to the standards. All products need not conform to existing standards, but the extent to which products are compliant must be understood. Generally, COTS and new products integrated into ECS systems demonstrate technical advantage when they are standards compliant. Standards compliance is not a subsystem design issue where limitations or capabilities are not essential; but knowledge of limitations, as provided by an assessment, is important.

5.10 Object-Oriented Design

Systems based on object-oriented data models originated with an object-oriented programming paradigm. The object-oriented programming paradigm subsumes the concept of abstract data types in programming languages. Abstract data type declarations explicitly define public and private portions of a data structure or an object. Abstract data types in object-oriented languages, called classes, encapsulate private data portions of the object with public procedures, called methods. Encapsulation is used to simplify program construction and maintenance through modularization. As long as the public interface definitions are not changed, an object may be defined as a black box that can be constructed and modified independently of the rest of the system. This ability to group data, or to encapsulate, is the primary risk mitigator when writing and maintaining system design software.

5.11 Software Optimization

If an analysis indicates that the software requires optimization, the organization’s best programmers should be assigned to the task. Optimization should be jointly performed by the programmer and the analyst. The programmer should determine the best approach to mitigate the problems, but the analyst should retain the right to veto any method demonstrated to be difficult to maintain. Optimized software is also easier to maintain in the operational environment.

Software should be optimized only after a particular program is completed. For the ECS object-oriented design, this means that optimization will occur frequently or after each module is completed. The goal of optimization is to modify that part of the module which will yield the greatest performance increase. Optimization of one small module, or subroutine, will enhance the program's speed considerably. Software code optimization techniques:

a. Use an optimizing compiler.

b. Record in assembly language.

c. Improve Input/Output (I/O) speed by changing file access methods, increasing buffer and block size, etc.

d. Replace routine calls with macros.

e. Combine modules.

f. Improve the modules' algorithms.

g. De-normalize files.

Standards in database systems foster interoperability and make it easier to write applications that can be converted across the spectrum of hardware systems. Software optimization and standards compliance increase interoperability in the ECS and are desirable for many reasons: better performance, reliability, support, operational availability, or availability of replacement products in the event that a vendor goes out of business. Standards are the ultimate guide for software optimization.

5.12 Integration and Testing

I&T is accomplished by testing individual ECS system functionalities that cross functional interfaces frequently. The thread build test approach, implemented as a risk mitigation concept, minimizes the requirement verification and simplifies problem resolution. For this approach, a thread (a set of software and hardware operational procedures) implements a function. Functions are identified by decomposition of requirements into threads allowing design-by-release flexibility, release schedule development, and integration and acceptance testing support. How ECS I&T was designed to mitigate risk may be reviewed in the System Integration and Test Plan of Interim Release 1 for the ECS Project, Volume 1, 402-CD-001-002, December 1994.

5.12.1 Testbed

The ECS testbed will emulate DAAC operational interfaces and capabilities. The testbed will be located in the STL and will consist of a 10 base T ethernet hub, an EP server, a planning and ingest workstation, a router and toolkit/algorithm workstation(s), and a Silicon Graphics computing capability (a processing host for the planning and data processing system). Emulating ECS operational capabilities will reduce the risks associated with the transition to Version 1 from Version 0. Operational interfaces with the DAAC sites can be simulated prior to transition to identify design deficiencies and to evaluate data conversion and operational procedures and concepts. All of these activities will minimize the risks associated with systems acceptance.

5.12.2 Independent Acceptance Test Organization

The functions performed by the Independent Acceptance Test Organization (IATO) are designed to minimize ESDIS program-level ECS risks. The IATO supports the Government Acceptance Test Team's (GATT) ECS performance evaluation. The IATO will assign a test manager to coordinate and run ESDIS-level acceptance testing. The IATO will also provide test conductors to execute the step-by-step procedures defined in the System Acceptance Test Procedures (DID 411/VE1). Test conductors write, collect, and track non-conformance reports and determine their impact on IATO test plans, scenarios, test cases, and procedures. In addition, the IATO provides benchmark tests to verify ECS system operational performance, and the acceptance testing procedures to be used to verify approved changes and enhancements. Their test scenarios drive

the IATO's evaluation of ECS software and hardware against established acceptance test criteria. Based on the GATT's recommendation, the COTR will determine a Release's acceptability. The IATO participates in the Release Readiness Review (RRR) after testing at all of the DAACs has been completed. At the RRR, the IATO presents the test results to the GATT.

The ESDIS Program Release will not be accepted until all ESDIS Level-1, or Critical, discrepancies at the ECS level have been corrected. Discrepancies classified as urgent or routine will be reviewed at the RRR to determine if they will prevent Release acceptance.

Level-3 requirements verification using operational scenarios is key to the IATO’s acceptance testing program. IATO operational test scenarios are oriented to ECS operations and management requirements. These scenarios are developed primarily by the IATO and address various operational concepts without emphasizing a specific user group. Operational test scenarios focus on areas such as spacecraft command and control, problem reporting and correcting, schedule adjudication, resource tracking, and security control.

The IATO will oversee segment- and system-level tests, will ensure that the tests are conducted thoroughly, and will review and evaluate the test results. The IATO will confirm that all Level-4 requirements have been tested fully and the results documented by the segment-level testing team. Mission-specific flight operations Level-4 requirements will receive particular attention. The confirmation process will selectively review test plans, results, and scenario (script) documentation.

Documentation related to system operation (user's manuals, operator's manuals, etc.) will be acceptance tested. All documents must be complete, accurate, and detailed. Document deficiencies will be noted for correction. Document errors, however, do not pose a serious threat to system operation and will not warrant Release rejection.

5.13 ECS Project Cost and Schedule Simulation Model

Subparagraph 5.8.2 discusses the Pugh-Roberts modeling technique and the results of the model-based analysis of the object-oriented development approach and cost integration. Additionally, subparagraph 8.5.2 reflects the correlation between the programmatic risks addressed in this document and those identified in the Pugh-Roberts analysis.

This page intentionally left blank.

6. Risk Identification and Estimation

6.1 Risk Taxonomy

Risk assessment was supposed to measure the degree of risk associated with risk items. This assessment was required to prioritize risk items and, subsequently, to measure the effectiveness of risk reduction and mitigation plans. Prioritization was successfully accomplished by grouping the risks into classes descriptive of ECS development processes. Broad classes of development activity selected for ECS risk assessment were related to user interaction with the ECS, and architectural, technological, evolutionary, systems operations, and programmatic risks. The following subparagraphs identify ECS risks by class and describe the classes.

6.1.1 User Interaction Risks

User interaction risks are associated with mutual or reciprocal action or influence between the ECS and the scientific community. These risks include the number and activity of users, the algorithm integration process, and the interoperability of Earth science data models.

6.1.2 Architectural Risks

Architectural risks are associated with achieving an organized and unified ECS structure or concept suggesting the proposed ECS architectural design. Architectural risks arise primarily because of interfaces with external systems. These risks involve an ECS interaction, schedule, and/or control function.

Examples of ECS architectural risks include the support approach for the GCDIS/UserDIS, (A-1), and Space Asset Safety, (A-3). These risks will be prioritized and addressed in later releases of this document.

6.1.3 Technological Risks

Technological risks result from ECS technical process improvements that increase productivity, performance, scalability, or maintainability while eliminating older processes. Technological risks are mitigated by assessing future predictions and evaluating technology. Examples of ECS technological risks include DCE Immaturity for Release A, (T-9), and CORBA Immaturity for Release B, (T-1). These risks will be prioritized and addressed in later releases of this document.

6.1.4 Evolutionary Risks

Evolutionary risks are associated with the various information services that the ECS should support or expect to accommodate in the future. Evolvability may be defined as system-wide areas that the ECS and applicable technologies and services could migrate to in the future. ECS evolutionary risks include the storage technology described in paragraph 7.11, Database Management Systems, (T-7).

6.1.5 System Operational Risks

System operational risks are associated with the performance of practical system work or involving the practical application of system principles or system processes. ECS system operational risks include the scope of ECS operations in the DAACs, automated operations in data distributions, and paradigm shifts in user support described in subparagraphs 3.3.2, 5.2.2, and 5.2.3.

6.1.6 Programmatic Risks

Programmatic risks are associated with program performance. These risks include all aspects of performance, planning, scheduling, and productivity. ECS programmatic risks include the compressed development schedule of paragraph 7.1, Compressed Development Schedule, (P-3).

6.2 Comprehensive Risk Identification

As a result of pre-contract activities and the ongoing ECS risk analysis, the risk items listed in paragraph 3.2 have been identified as relevant to the ECS Project.

6.3 Estimation Process

The estimating process is accomplished by interviewing knowledgeable ECS personnel, scoring risk information, and classifying the risk.

6.3.1 Interview Process

Typically, the interview process is a discussion between a risk facilitator and project personnel to collect risk information. The interview process is an informal discussion with personnel from the discipline associated with the risk. The discussion may include managers, engineers, Reliability, Maintainability, and Availability (RMA) personnel, configuration management personnel, or other personnel knowledgeable of the subject risk. The facilitator follows a list of subjects designed to collect relevant data about the risk. Frequently discussed subjects are risk reduction, risk transference, resource reservation, and risk assumption. Other subjects may include risk aversion, implementation, monitoring, identification, assessment, and analysis.

6.3.2 Scoring

The collective interview process results are instrumental in scoring, or prioritizing, the ECS risk. Relevant data is used to determine risk scoring and estimation probability and consequences as described in subparagraph 4.2.3, Risk Estimation.

6.3.3 Isometric Risk Plot

The Isometric Risk Plot is a representation of the risk consequence and probability of failure plotted on a coordinate axis. As consequence and probability increase on the scale, the likelihood of event occurrence increases. Thus, as the probability of failure increases, the risk increases. Likewise, as the consequence of failure increases, the likelihood of occurrence increases. From

this information, a graphical plot of the risk factors may be derived. The greater the risk factor numerically, the higher the risk. A plot of the risk factors may be scaled as low, medium, or high.

To establish the priority risks, a cut-off level may be set arbitrarily to represent risk priority. For example, all risks above a level of 3.8 are considered high risk items. Priority risks typically represent a cost, schedule, or resource impact inconsistent with ECS Project goals.

6.4 Identified Priority Risks

The ECS environment supports a large number of risk items with limited available risk management resources. Generally, 80 percent of a program's risks result from only 20 percent of the perceived risk items. Prioritizing risk items identifies the top 20 percent of the risk items selected to receive risk management resources. The following ECS risk items have been ranked in the top 20 percent by a quantitative and qualitative risk assessment process.

a. Programmatics
    1. Compressed Development Schedule**,** (P-3).
    2. Operations Concept and Multi-Segment Integration, (P-7).
b. Systems Operation
    1. Production Planning and Scheduling, (S-7).
c. Architecture
    1. COTS Full Lifecycle Cost and Management, (A-6).
    2. Communications Service System Overhead, (A-7).
d. Technology, Communications
    1. Object Management Framework Availability, (T-10).
    2. CSMS Service by Platform, (T-11).
e. Storage Technology
    1. Cost-Effective Storage Technology**,** (T-5).
    2. COTS Hierarchical Storage Management**,** (T-4).
    3. Archive Scalability and Maintainability**,** (T-8).
    4. Database Management Systems, (T-7).
f. User Interaction
    1. Number and Activity of Users, (U-1).
    2. Processing and Storing Standard Products, (U-4).

This page intentionally left blank.

7. Priority Risk Evaluation

This section details the risk evaluations for items on the prioritized risk list (refer to Table 7-1). The prioritized risk list was determined, as described in Section 6, by estimating the priority of each item on the comprehensive risk list. The risk evaluation process is described in detail in paragraph 4.2. Section 7 discusses the high priority risks in detail, including current assessments.

The risk evaluation method described in this section is more involved than the estimation process described in Section 6. In particular, this evaluation method develops the following four main risk evaluations for each high risk item:

a. Risk Description. A detailed risk description is developed, starting with the description developed during risk estimation.

b. Evaluation Criteria. The risk's consequences and probability are described. If possible, exposure from the risk is estimated as a dollar value. This justifies mitigation plan expenditures.

c. Risk Mitigation Plans. Risk mitigation plans are described. Mitigation expenses and resources are justified using the calculated risk exposure. Objective criteria (monitoring variables) are identified to evaluate risk reduction resulting from mitigation plans. Target values indicative of success are identified.

d. Contingency Plans. Contingency plans are described. Events or the limits of monitored variables triggering contingency plan implementation are identified.

The PDR further categorized the priority risks as System Development, Infrastructure, Archive Storage, or Push and Pull risks. Table 7-2 reallocates priority risks for design and presentation purposes, but does not list them sequentially. Many of the risk activities overlap and are interrelated.

Risk evaluations are developed by an ECS RMP member and presented to the panel for discussion. The RMP discussion provides risk evaluation refinement, risk acceptance, and awareness across the program. Paragraph 4.1 describes the RMP process in detail.

Mitigation plans are identified for each high priority risk item. Prototypes and studies are the two main mitigation approaches. Table 7-3 summarizes the prototypes which are mitigation plans for priority risk items. Tables 7-4 through 7-6 summarize the studies which are mitigation plans for priority risk items.

For a general discussion of the prototypes, studies, models, and white papers referred to in subsequent paragraphs, refer to current issues of the following documents:

a. 211-CD-001, Prototyping and Studies Progress Report for the ECS.

b. 311-CD-003, CSMS Database Design Specification for the ECS.

c. 318-CD-000-xxx, Prototyping and Studies Progress Report for the ECS.

Table 7-1. Prioritized Risk List

Number	Risk Title	Exposure ($K)
	Programmatic	
P-3	Compressed Development Schedule	7,000
P-7	Operations Concept and Multi-Segment Integration	TBD
	System Operations	
S-7	Production Planning and Scheduling	TBD
	Architecture	
A-6	COTS Full Lifecycle Cost and Management	TBD
A-7	Communications Service System Performance Overhead	TBD
	Communications and Storage Technology	
T-11	CSMS Service by Platform	TBD
T-5	Cost-Effective Storage Technology	11,750
T-4	COTS Hierarchical Storage Management	TBD
T-8	Archive Scalability and Maintainability	TBD
T-7	Database Management Systems	TBD
	User Interaction	
U-1	Number and Activity of Users	TBD
U-4	Processing and Storing Standard Products	TBD

Table 7-2. Reallocated Risk List

Number	Risk Title
	System Development
P-3	Compressed Development Schedule
P-7	Operations Concept and Multi-Segment Integration
A-6	COTS Full Lifecycle Cost and Management
	Infrastructure
T-11	CSMS Service by Platform
A-7	Communications Service System Performance Overhead
	Archive Storage
T-4	COTS Hierarchical Storage Management
T-5	Cost-Effective Storage Technology
T-8	Archive Scalability and Maintainability
	Push and Pull
U-1	Number and Activity of Users
S-7	Production Planning and Scheduling
T-7	Database Management Systems
U-4	Processing and Storage of Standard Products

Table 7-3. Prototypes Mapped to Priority Risk Items

Prototypes Related to High Priority Risks	High Priority Risks											
	Program.	Communications Technology				Storage Technology				User Interaction		
	P-3 Dev. Schedule	T-9 DCE for Release A	T-1 CORBA - Release B	T-10 Object Mgmt. Fr'mwork	T-6 Perf. of Comm I/F	T-5 Cost Effective Storage	T-4 COTS HSM	T-8 Scale & Maintain Archive	T-7 DBMS Perf.	U-1 Number & Activity of Users	U-4 Standard Products	U-2 Interop of ES Data Models
In Progress Prototypes												
Collaborative Prototyping Testbed		•	•		•					•		•
DCE Encapsulation Prototype		•	•									
Data Dictionary and Vocabularies												•
Data Processing Prototype											•	
Data Type Services									•			
ECS-HDF Standards								•				•
Internet Performance Characterization Study					•							
Interprocess Communications Prototype		•										
Local Information Manager									•			•
Network Management Prototype				•								
ORB Prototyping			•									
Science Software Execution Prototype											•	
Completed Prototypes												
Advertising Service		•	•									
DCE/DME Products (COTS Evaluation)		•		•								
DCE/DME Prototype & Mitigation		•		•								
Develop Archive System w/ Science Data						•	•					
Evaluate Archive Media/Recorders						•	•					
Evaluate Archive Robotics Unit						•	•	•				
File Manager							•					
Multi - FSMS Product Integration Evaluation							•					
Spatial Data Access												•
Proposed Prototypes												
Earth Science Language and Protocols												•
MSS Application Prototyping				•								
MSS Prototyping				•								
ORB and Object Service Abstraction		•	•									
Trader/Advertising Prototype		•	•									

Table 7-4. Studies Mapped to Priority Risk Items

Studies Related to High Priority Risks (document number listed if applicable)	High Priority Risks									
	Program.	Communications Technology			Storage Technology				User Interaction	
	P-3 Dev. Schedule	T-9 DCE for Release A	T-1 CORBA - Release C	T-10 Object Mgmt. Fr'mwork	T-5 Cost Effective Storage	T-4 COTS HSM	T-8 Scale & Maintain Archive	T-7 DBMS Perf.	U-1 Number & Activity of Users	U-4 Standard Products
PDR Technical Baseline (1/9/95)	•								•	•
ECS Release Plan Content Description (FB9403V4, 9/94)	•								•	
ECS Release Plan Capabilities Mapping Table (FB9403V4, 9/94)	•								•	
DAAC Facility Impact Analysis for Science Data Product Generation (JU9404V1)										•
User Studies										
User Characterization and Requirements Analysis (19400312)									•	
ECS User Characterization Methodology and Results (19400313)									•	
User Scenario Functional Analysis (19400548)									•	
ECS Scientist User Survey (ESUS) (19400549)									•	
Independent Architecture Studies										
GMU Independent Architecture Study					•			•	•	
UCB Independent Architecture Study						•		•	•	
UND Independent Architecture Study									•	

Table 7-5. Studies Mapped to Priority Risks - SDPS

Studies Related to High Priority Risks (document number listed if applicable)	High Priority Risks									
	Program.	Communications Technology			Storage Technology				User Interaction	
	P-3 Dev. Schedule	T-9 DCE for Release A	T-1 CORBA - Release C	T-10 Object Mgmt. Fr'mwork	T-5 Cost Effective Storage	T-4 COTS HSM	T-8 Scale & Maintain Archive	T-7 DBMS Perf.	U-1 Number & Activity of Users	U-4 Standard Products
In-Process Studies										
FSMS Implementation						•	•			
Network Attached Storage Technologies							•			
COTS DBMS Evaluations								•		
Reprocessing Paradigm Impacts on Production										•
Selection of Products for On Demand Processing									•	
Hardware Technologies for Permanent Data Storage					•					
Physical Access Media Management						•				
Storage Technology Insertion					•		•			
Data Dictionary /Vocabulary COTS								•		
Production Topologies										•
Production Platform Families										•
Science Software Direct Access to Data Server									•	
Distributed and Parallel Processing										•
ECS HDF Standard										•
HDF Storage Issues for the ECS Project										•
I/O (HDF) Efficiency										•
Proposed Studies										
User Supplied Processing Methods										•
Completed Studies										
Data Compression Study (19400316)					•					
File Manger Study						•	•			
Evaluate Archive Media/Recorders					•	•				

Table 7-6. Studies Mapped to Priority Risk Items - CSMS

Studies Related to High Priority Risks (document number if applicable)	**High Priority Risks**									
	Program.	**Communications Technology**			**Storage Technology**				**User Interaction**	
	P-3 Dev. Schedule	**T-9 DCE for Release A**	**T-1 CORBA - Release C**	**T-10 Object Mgmt. Fr'mwork**	**T-5 Cost Effective Storage**	**T-4 COTS HSM**	**T-8 Scale & Maintain Archive**	**T-7 DBMS Perf.**	**U-1 Number & Activity of Users**	**U-4 Standard Products**
In-Process Studies (540-TP-001-001)										
Management Agents				•						
Selection of Management Framework Architecture and Product Selection				•						
Agent Configuration for a Typical Host				•						
DCE Cell Configuration		•								
DCE Encapsulation Trade Study		•	•							
Proposed Studies										
Presently none										
Completed Studies										
DCE/DME COTS Evaluation White Paper (19300561)		•								
DME Migration Study (19300632)		•								
CORBA Object Request Broker Survey (MR9408V1)			•							

7.1 Compressed Development Schedule, (P-3)

7.1.1 Risk Description

Compression of the ECS development schedule based on delayed start, early launches, and SRR recovery resulted in excessive peak development manpower requirements for previous Release functionality assignments. Mitigation includes detailed planning of the Release Schedule's content, reallocation of Release functionality, hiring and training, and applying our incremental development and thread build integration approach to the project (see Figure 3-1). Concerns include the following:

a. Compressed development may require excessive peak manpower to achieve assigned functionality for defined Release dates.

b. Comparison with other Hughes programs of similar size raises questions of ECS's ability to develop the code - SDPS 237 Thousand Single Lines of Code (KSLOC) (IR1 69 + Release A 168) in 21 months.

c. The Tropical Rainfall Measurement Mission (TRMM) launch is firm (refer to Kleinberg).

7.1.2 Evaluation Criteria

Evaluation criteria for a compressed development schedule include an assessment reflecting the following cost overrun based on the equation:

Cost Overrun = heads over baseline * cost/head.

Peak manpower and cumulative hours were estimated as follows:

Comparison to other Hughes programs indicates that, with 237 KSLOC, an additional 10 to 12 months of programming effort will be required. (5 months at $5M/month ~ $25M, 35 percent probability, $7M exposure). To maintain the existing schedule, a reduction by SDPS to 150 KSLOC will be required.

Compressed development schedule evaluation for the system development must be completed and the risks must be mitigated by the Release Initiation Review (RIR) for Release B.

7.1.3 Risk Mitigation Plans

Risk mitigation plans for a compressed development schedule include: development effort modeling, potential development content changes, manpower assessments, Release prioritization, and focus teams.

ECS has modeled the development effort and will continue to reassess the development schedule and provide estimates as follows:

a. Lines of Code (LOC) Estimates by Release. This information will be incorporated into each IDR update.

b. Schedule Modeling. The modeling estimate reflected a 10 percent budget overrun and 1 week slack in Release A after moving 28 KSLOC (18 KSLOC from SDPS, 10 KSLOC

from CSMS) from Release A to Release B and Version 0 Client (29 KSLOC). Input to the model was provided by Smith and Parag of ECS.

c. COTS Integration Estimation [System Evaluation and Estimate of Resources (SEER)-System Element Management (SEM)].

Schedule content changes and development activity considerations include:

a. Reuse the Version 0 Client in Release A.

b. Maximize COTS content through a COTS-intensive trade study. Trade study results should inform COTS selection guidelines to be used by all segments in all design analysis efforts.

Manpower and the skill mix are to be monitored as follows for maximum productivity:

a. In the event that the model's projections are proven accurate, a shift in existing personnel will be employed to complete the new skill mix. Additional personnel will be employed (hired) only in the event that ECS cannot support a mission (flight project) schedule. The development schedule will be monitored for indications of potential impact.

b. COTS vendors will be solicited to provide COTS product I&T support.

Prioritization and reassessment of Release A requirements may potentially mitigate schedule impact as follows:

a. Automated ESDIS capabilities could be delayed or traded for manual O&M procedures.

b. Segment-to-system I&T hand-off reassessment may compress or eliminate overlapping test activities.

c. The duration indicated by the model between the Test Readiness Review (TRR) and the Consent to Ship Review (CSR) may be reduced by 30 percent.

d. Specialized management (focus) teams will isolate and emphasize development activity and minimize schedule impact through intense schedule management efforts.

A final risk review and assessment by the ECS Project RMP will be completed by Release B, RIR.

7.1.4 Contingency Plans

Risk mitigation contingency plans for a compressed development schedule include assignment of approximately 100 to 120 LOC per man month (LOC/mm) to Track 2 development. Additionally, the delivery schedule will be tracked to verify that the schedule can be met. The LOC/mm delivered to test will be tracked at an approximate level of 48,000 to 50,000 LOC/mm. Contingency plans are assigned based on the following:

a. IR1 productivity < TBD LOC/mm, ... (TBDs are determined by a SEER model assessment.).

b. EP 6 productivity < TBD LOC/mm, ... (Results from EP 6).

c. Release A productivity < TBD LOC/mm.

d. Release A development of operational procedures (O&M) including: manual-intensive operations, a go or a no go at the Release A CDR, and a high cost and head count.

7.2 Operations Concept and Multi-Segment Integration, (P-7)

7.2.1 Risk Description

Operations concept and multi-segment integration risks result from the lack of a refined, documented system usage operations concept enabling the customer and user community to verify the subsystem design and to understand how the segments might be integrated into an operable system. The risk, shared by ECS and ESDIS, is that with the DAACs' operational activities already established, changes to existing DAAC site policies may be resisted. Where policy and procedure differ, ESDIS shares the responsibility to direct ECS and DAAC integration.

Development of an ECS operations concept consistent with successful DAAC operations is a difficult task and may require considerable ECS and DAAC operations management flexibility. Difficulties arise when operational scenarios are not consistent with established DAAC policies and operational procedures. Any perception that operational concepts and scenarios represent a change to established operational activities at the DAAC may engender resistance. That the DAAC databases will be integrated is inevitable. Such a change would occur without the ECS. The operations scenarios conceptualize the ECS as the central focus (refer to DID 604). This focus represents the ECS as central, but does not necessarily require a change to the established DAAC operating procedures. Currently successful DAAC procedures are more than acceptable in the ECS environment and will continue to be used.

7.2.2 Evaluation Criteria

Operations concept and multi-segment integration evaluation criteria include a review of the third release of the Operations Concept Document for ECS, DID 604/OP1, and its acceptance as representative of the activity necessary to accomplish ECS operations. Furthermore, the document will present the procedural activities necessary to illustrate multi-segment integration as defined in ECS Internal ICDs, DID 313/DV3, and will include:

a. Access and privilege control.
b. Process and process communication.
c. Data file transfer.
d. Multiple transaction request.
e. Accessing the host on a Local Area Network (LAN) or Wide Area Network (WAN).
f. Network access.
g. NASA Science Internet (NSI) connectivity.

System integration and acceptance tests will further evaluate and validate the operations concepts and multi-segment integration from a thread build approach. The system development operations concept and multi-segment integration evaluation must be completed and the risks must be mitigated by the RIR for Release B.

7.2.3 Risk Mitigation Plans

Operations concept and multi-segment integration risk mitigation plans include:

a. Operations Concept Document for ECS, CDRL DID 604/OP1.

b. Detailed design scenarios.

c. Operations teleconferences.

d. Operations scenarios.

The Operations Concept Document has been submitted for review and assessment three times. Considerable RID and work-off activity have been required. Currently, detailed scenarios satisfying multiple DAAC site and user operational methodologies are documented. The ECS system design will meet all of the Level-3 requirements. Each of these requirements is traceable to ESDIS Level-2 requirements identifying high-level operational interfaces between the ECS and the DAAC sites. Level-3 requirements are simple capabilities that the ECS must possess. Operational activities that the DAACs may choose to implement for day-to-day product request deliveries are numerous. Thus, the operations concept scenarios documented represent to the DAACs and the user community only one available view of how operational requirements may be satisfied.

Detailed design scenarios illustrating how system users may apply segment capabilities to common and repetitive activities will be documented. These scenarios will demonstrate to the user how to initiate activity across low-level segment interfaces and how to accomplish tasks requiring the interaction and integration of multiple subsystems.

The ECS design does not require continuous human interaction to provide data to the user community. Initially, this digitally interactive process may be unfamiliar to some members of the user community. If a user is not familiar with documented procedures or the ECS capabilities, telecommunications and a support desk will be available to resolve questions and “operator” difficulties. This service probably will not continue for the life of the ECS. Documented operational scenarios on an electronic bulletin board will establish policies and procedures for ECS use. Questions of policy, training, authorization, system access, etc., will be available electronically.

7.2.4 Contingency Plans

Operations concept and multi-segment integration risk contingency plans include test cases identified in System Integration and Test Plans for ECS, Volume 1, 402-CD-001-002, for IR1 and Volume 2 for Release A. Test cases are performed at the system level, validating a segment services function. These test cases validate ECS operational capabilities across segments. Refer to the subject document for detailed procedures.

7.3 COTS Full Lifecycle Cost and Management, (A-6)

7.3.1 Risk Description

COTS full lifecycle cost and management risks include the potential to underestimate the actual cost of COTS in the following areas: integration “glue code”, configuration effort, and maintenance upgrades and operations. Mitigation activity results and the true COTS cost will be released in March 1995.

7.3.2 Evaluation Criteria

COTS full lifecycle cost and management evaluation criteria include a management strategy developing the following evaluation metrics:

a. Number of COTS installations.

b. Number of DAAC-specific configurations.

c. Functional coverage (functions and interface).

d. Partial functional coverage (functions and interface).

e. Glue software required.

f. Applicability.

g. COTS maturity.

h. Learning and configuring COTS.

i. COTS installation labor.

j. Re-installation labor.

k. Release frequency.

l. Average COTS maintenance support required.

m. New technology and evolutionary impact.

Specific parameters for each set of the listed criteria rate the labor cost as high, moderate, or low. This data is then summarized to determine the product's lifecycle cost.

Other information essential to the evaluation includes the name of the segment using the COTS product, the name of the Level-4 function using the COTS product, the name of the COTS product, the name of the COTS vendor, and the ECS code assigned to the product.

The COTS full lifecycle cost and management system development evaluation must be completed and the risks must be mitigated by the RIR for the Release B design.

7.3.3 Risk Mitigation Plans

COTS full lifecycle cost and management risk mitigation plans include:

a. A COTS cost evaluation metric.

b. Single Lines of Code (SLOC) estimates including “glue” and configuration effort.

c. A COTS prototype approach.

d. COTS maintenance (provided by O&M).

e. SEER- and Boehm-based models.

The actual cost of COTS products over the lifecycle was considered in two parts. Development estimates included COTS-related efforts, and modeling efforts were re-evaluated and refined over time as candidate COTS products were better understood. Development I&T, familiarization, and configuration were considered also. As a result of these factors, greater data definition, scripts, and “glue” code were included in the SLOC. Prototyping demonstrated how and to what degree the COTS products met ECS requirements. Prototype assessment reports documented the features and capabilities of each product considered and determined the technology and product selected. The O&M sustaining engineering staff evaluated the products and effort required for long-term operations, maintenance, installation, and COTS upgrade I&T.

An ongoing process is used to re-evaluate and refine the estimation model. This process includes developing the following metrics to quantify required COTS integration efforts: additional COTS product integration software, applicability, product maturity, learning curves, configuration efforts, installation costs, re-installation labor, release frequency and interval, and maintenance support. Data from these metrics will be modeled to identify associated costs. SEER and the ECS development cost model will receive the data. COTS products will be evaluated in this manner over the life of the ECS.

A final risk review and assessment by the ECS Project RMP will be completed by Release B, RIR.

7.3.4 Contingency Plans

There are no additional risk contingency plans for COTS full lifecycle cost and management. All efforts to mitigate the risks associated with using COTS in the ECS are being implemented. The COTS full lifecycle cost and management activity will be monitored according to the metrics stated in subparagraph 7.3.2. When cost and management projections exceed the established metric value, ECS project management will determine the COTS expenditure cost/benefit and prudent course of action.

7.4 CSMS Service by Platform, (T-11)

7.4.1 Risk Description

CSMS service by platform risks include a failure to identify the platform. That is, the platform [DCE, Object-Oriented DCE (OODCE), etc.] to be supported with CSMS services in IR1 and Release A must be identified. Platform selection will be announced formally at CDR. Internally, the decision should be made in May 1995. Considerable platform selection effort has been expended since the beginning of the project. Each platform's maturity and robustness, sheltering the SDPS and FOS during the migration from DCE to CORBA, DCE's suitability as a transport service beneath CORBA, and the risks associated with using CORBA in Release A have been

investigated. These and other related questions are fully understood. The tendency is to delay platform selection for as long as possible, hoping that the platforms considered will mature enough to totally mitigate the associated risks.

7.4.2 Evaluation Criteria

Platform selection is related to the ECS infrastructure, which includes DCE, CORBA, Distributed Management Environment (DME) 3.0 (OMF), and Object Service Maturity. CSMS service by platform evaluation criteria include:

a. Standards compliance.

b. Product availability and time frame.

c. Interface application, custom versus standard.

d. Product portability.

e. Migration of the DCE to CORBA.

f. Development costs.

g. Software support costs.

The CSMS service by platform infrastructure finalization evaluation must be completed and the risks must be mitigated prior to the CDR for Release A.

7.4.3 Risk Mitigation Plans

CSMS service by platform risk mitigation plans include performing a trade study analysis of the available products against the listed criteria. Specifically, the trade/studies will evaluate DCE for IR1, and OODCE for Release A. The current tendency is to use DCE, a widely accepted and proven platform. A final risk review and assessment by the ECS Project RMP will be completed by Release A, CDR.

7.4.4 Contingency Plans

The CSMS service by platform contingency plan is to assess the following options as possible solutions:

a. Custom encapsulation of DCE by a CSMS code to provide an Object Management Group (OMG) Interactive Data Language (IDL) interface and thereby establish an ECS services standard. This was the SDR baseline.

b. CORBA 1.1 Object Request Broker (ORB) custom-ported to DCE. Extensions for required additional services would have to be written. Single-vendor, multi-platform ORBs exist written to the CORBA 1.1 standard. Extensions are not yet available. Hewlett Packard (HP) and Digital Electric Corporation (DEC) ORBs do not fully meet ECS requirements. Within the next 6 months, DEC may provide a release of Object Broker that runs over DCE. The HP and DEC products must not be considered viable, because they are both unavailable.

c. OODCE, HP’s object-oriented DCE product. OODCE, a development tool and run-time library, provides a commercial class library, an OMG-like IDL, and an IDL-to-C++ compiler. The OODCE development software is licensed; run-time copies are distributed without licenses.

d. OODCE, a Hitachi object product that runs over DCE and provides IDL auto-generation, has not yet been released.

e. Modified class libraries. CSMS could select a commercial C++-class library designed for a sockets environment and custom-port and extend the commercial-class library to a DCE environment.

7.5 Communication Service System Performance Overhead, (A-7)

7.5.1 Risk Description

CSS performance overhead risks are related to wrapping OODCE Objects with OMG/CORBA interfaces and to CSS performance. OODCE enables developers to build object-oriented DCE applications by automating the packaging of DCE services as C++ objects. OODCE encapsulates much of the complex DCE syntax and many of its commands into powerful, easy-to-use objects. However, this encapsulation affects performance and may not meet system performance requirements.

Standards compliance will facilitate the transition from DCE to CORBA. The encapsulation technique chosen should present a standards-based interface to ECS applications. In the ECS, the natural standard of choice is OMG IDL.

7.5.2 Evaluation Criteria

CSS performance overhead evaluation criteria include the following:

a. Schedule and cost.

b. Availability.

c. Standards compliance.

d. Portability.

e. Software support.

The CSS performance overhead infrastructure finalization evaluation must be completed and the risks must be mitigated prior to the CDR for Release A.

7.5.3 Risk Mitigation Plans

CSS performance overhead risk mitigations plans include:

a. IR1 evaluations.

b. Interface definitions in the Programmer's Guide.

c. CSS performance testing [sockets and Remote Procedure Calls (RPC)].

d. DCE Distributed File System (DFS) and Network File System (NFS) performance evaluation.

A review of vendor-released products revealed that only HP offered an encapsulation product running on top of DCE. This released product was brought in house for prototyping in July 1994. In the prototype of the product's capability, the encapsulation method's performance was measured. This prototype included:

a An object reference passing over DCE (verified with a simple CSS).

b. An advertiser/trader function.

c. A joint SDPS/CSMS advertiser/trader.

d. Joint FOS/CSMS interprocess communications.

The interface definitions in the Programmer's Guide are *de facto* standards established for the ECS interfaces. The definitions became necessary because many key OMG services have not yet been standardized; their interfaces could only be extrapolated from dynamic snapshots of work in progress, competing products, and prototype products. These extrapolations and available data will be used to establish optional interface definitions.

7.5.4 Contingency Plans

CSS performance overhead contingency options include:

a. Custom development (and resulting schedule risk).

b. Custom ports of ECS-specific software (to other platforms).

Only the OODCE option provides full vendor maintenance. DCE is on a roughly annual update cycle, which is a significant advantage. The other solutions involve custom software and/or custom ports, requiring extensive maintenance programs at additional cost to ECS. Other options include DFS and NFS. Currently, DFS lacks some required data server performance capabilities.

7.6 COTS Hierarchical Storage Management, (T-4)

7.6.1 Risk Description

The fundamental COTS HSM risk is that HSM functions are not designed for ECS-class supercomputing applications. HSM functions are designed to extend the capacity of disk-based NFSs, which have moderate storage and I/O volumes and application-independent secondary storage management capabilities.

HSM is not scalable to support the multiple supercomputing applications of the larger DAACs, would cause I/O bottlenecks because it is not designed to support millions of files, and would produce unacceptable secondary/tertiary storage ratios. Additionally, because formats are proprietary, there is no standard storage format; the market for ECS HSM is very small; and some HSM COTS products raise the following reliability and performance concerns:

a. COTS storage management and distributed file systems may not be reliable.

b. HSM functions may limit system performance.

7.6.2 Evaluation Criteria

COTS HSM evaluation criteria include the following:

a. Storage volumes must exceed 1 Terabit (TB) throughput with a capacity growing to 3 Petabytes (PB).

b. I/O volumes.

c. Secondary storage management shall be application independent.

The COTS HSM evaluation must be completed and the risks must be mitigated prior to the CDR for Release A.

7.6.3 Risk Mitigation Plans

COTS HSM risk mitigation plans include partitioning the storage design into scalable, low-risk components, avoiding the HSM archive bottleneck. Volume and robotics management will be separated from the high bandwidth I/O transfer. Also, the data server architecture will support the File and Storage Management System (FSMS) replacement with a multi-FSMS approach. Risk mitigation strategies include the following:

a. Design HSM functions eliminating archive bottleneck. Use a file manager and archive system developed with science data.

b. Develop a multi-FSMS prototype. Evaluate product integration and archive media and records.

c. Develop a network-attached storage prototype. Evaluate the archive robotics unit.

7.6.4 Contingency Plans

COTS HSM contingency plans include reassessing the HSM approach. The design must be partitioned to include scalable, low-risk components. The options include waiting for technology to mature or developing custom code to integrate volume and robotics management, high bandwidth I/O transfer, secondary storage management, and user access services. In addition, custom software would have to be developed to provide rolling data ingest storage for approximately 1 year [or for Land Satellite (LandSat)-7, 30 days].

7.7 Cost-Effective Storage Technology, (T-5)

7.7.1 Risk Description

Cost-effective storage technology risks are associated with archive component media and form factors influencing PB storage. Each DAAC's planned floor space raises other issues. The following risks are identified:

a. Storage costs given capacity, performance, and RMA requirements.

b. Floor space allocated for equipment.

7.7.2 Evaluation Criteria

Cost-effective storage technology is a cost comparison issue. List purchase prices and Read-Only Memory (ROM) calculations for an Automated Tape Library (ATL) and media (only) were considered. Lifecycle cost was not calculated. Calculations included:

a. Baseline allocation for a 2.7 PB archive: $4,500,000.

b. Baseline recalculation using a homogeneous 2.7 PB Storage Tek (STK) archive: $18,500,000.

c. Homogenous 4.2 PB STK archive: $28,000,000.

d. Homogenous 22.7 PB STK archive: $112,000,000.

Risk exposure was calculated as follows: ($28M - $4.5M) *50% (Estimated likelihood) = $11.75M.

The cost-effective storage technology evaluation must be completed and the risks must be mitigated prior to the CDR for Release A.

7.7.3 Risk Mitigation Plans

Cost-effective storage technology mitigation plans include staying abreast of storage technology market developments and end-user applications, including Department of Defense (DoD), oil industry, and other science [e.g., European Laboratory for Particle Physics (CERN)] applications. Network-attached storage and data compression prototypes will develop storage volume reduction design concepts. The following items are related to these activities:

a. Storage Technology Insertion Plan.

b. Data compression prototype.

c. Network-attached storage prototype.

7.7.4 Contingency Plans

The cost-effective storage technology contingency plan is to store data on tape. A contingency plan for archive technology decisions will be developed from the following trade studies (an update will be based on the tape market assessment):

a. Network-attached storage technology.

b. Hardware technologies for permanent data storage.

c. Storage technology insertion.

d Compression within the archive.

7.8 Archive Scalability and Maintainability, (T-8)

7.8.1 Risk Description

The risk associated with archive scalability and maintainability is that a single computer cannot handle an arbitrary I/O load, especially supporting pull side performance. One major mitigating factor is the investigation of network-attached storage. For maintainability, it is critical to use proven robotics technology and to pursue the use of non-contact media technologies (e.g., serpentine tape). Issues include:

a. Current systems may not be scalable.

b. Large, long-lived archives may not be easily maintained.

c. Smaller system approaches are not viable for ECS.

7.8.2 Evaluation Criteria

Archive scalability and maintainability evaluation criteria include the following:

a. Storage volumes must exceed 1 TB throughput with a capacity growing to 3 PB.

b. I/O volumes.

c. Secondary storage management shall be application independent.

The archive scalability and maintainability evaluation must be completed and the risks must be mitigated prior to the CDR for Release A.

7.8.3 Risk Mitigation Plans

Archive scalability and maintainability risk mitigation plans include the following:

a. Develop a network-attached storage prototype using ECS Hierarchical Data Format (HDF) standards.

b. Use proven robotics technology. Evaluate the archive robotics unit.

c. Pursue non-contact media technologies (e.g., serpentine).

7.8.4 Contingency Plans

Archive scalability and maintainability contingency plans include reassessing the HSM approach. The design must be partitioned to include scalable, low-risk components. The options include waiting for technology to mature or developing custom code to integrate volume and robotics management, high bandwidth I/O transfer, secondary storage management, and user access services. In addition, custom software would have to be developed to provide rolling data ingest storage for approximately 1 year (or for LandSat-7, 30 days).

7.9 Number and Activity of Users, (U-1)

7.9.1 Risk Description

Accurate pull side user estimates are difficult to attain. The ECS is unique, and evolution of user interaction is anticipated. Estimates are necessary to size the data management, data server, and Internet working subsystems. Estimating the pull side user community entails risk. Who the users will be and what their usage patterns will be are estimates. Predictions of use based on past experience may be inaccurate due to the evolution of user methods. Inaccuracies in estimating the number and activity of users affect several areas of the system, including the inter-site traffic dependent on data set usage.

7.9.2 Evaluation Criteria

The evaluation criteria used to assess potential ECS Project impact include:

a. Scaled predictions of usage based on past experience.

b. Expected system usage evolution.

c. Inter-site traffic dependencies.

Applying evaluation criteria to a fluid and dynamic user/data model is definitely complex. To reduce this complexity, and as a result of cost factors identified in modeling studies, only the science user model is considered for this risk assessment and for evaluation criteria application. Specific data used to support the evaluation may be found in the Projected System Access and Utilization package presented at the June 1994 SDR. Copies of the document are in the Technical Baseline.

The number and activity of users evaluation must be completed and the risks must be mitigated prior to the IDR for Release B.

7.9.3 Risk Mitigation Plan

Risk mitigation plans for the number and activity of users include continued development of user, data, and system performance models; increased interaction with the Science Computing Facilities (SCF) and the larger EOS community through the EOSDIS prototype; and conducting design studies to reduce the design's sensitivity to variations in the actual number of users. Activities include:

a. User/data modeling.

b. Performance modeling.

c. EOSDIS prototyping using a collaborative prototyping test bed.

d. Conducting a processing versus storage trade study.

e. Performing a system design sensitivity analysis.

7.9.4 Contingency Plans

Contingency plans for the number and activity of users project a 20 percent scalability factor. This unanticipated increase in activity must be planned for logistically, in the event that rough order of magnitude estimates are inaccurate.

7.10 Production Planning and Scheduling, (S-7)

7.10.1 Risk Description

Production planning and scheduling risks include a COTS implementation that may not meet requirements for Release B planning and scheduling. COTS products do not necessarily consider the down time and maintenance anticipated in the ECS environment.

7.10.2 Evaluation Criteria

Production planning and scheduling evaluation criteria demonstrate the products' responses to ECS planning and scheduling requirements, including unscheduled equipment and software down time and maintenance. At a minimum, planning and scheduling capabilities should include:

a. Re-schedule tasks.

b. Restart tasks.

c. Execute local tasks (jobs).

d. Identify, launch, and monitor unscheduled tasks.

e. Manually intervene (i.e., the operator can manually impose schedule and time constraints).

f. Log messages and alert operators.

g. Display job dependencies between sites at multiple processing levels (i.e., by site, job group, or individual job dependency).

h. Maintain job information and status.

i. Differentiate levels of security.

j. Generate resource utilization reports.

k. Support system scalability and evolvability.

The production planning and scheduling system development evaluation must be completed and the risks must be mitigated by the IDR for the Release B design.

7.10.3 Risk Mitigation Plans

Production planning and scheduling risk mitigation plans include:

a. Planning and scheduling prototypes.

b. A planning and scheduling workshop.

c. Development effort risk accounts.

d. A survey of the commercial market for a viable COTS planning and scheduling package.

A COTS package with the planning and scheduling capabilities specified by the appropriate Level-3 and -4 requirements must be procured. If such a product is not currently available, the product featuring the most desirable capabilities will be selected. The ECS Project will develop code to provide the missing capabilities and the necessary "glue" for integration.

The Delphi Toolkit planning and scheduling prototype is currently being evaluated for its ability to generate a production plan. The tool can develop a multi-day planning schedule using predicted multiple downloads of Version 0 and ancillary data. The tool also accepts resource changes during operation. The tool should be able to accept down time and maintenance interruptions.

Current activities include workshops to discuss the planning, scheduling, and provisions for the service. The CSMS and the SDPS are considering a combined scheduling concept. This would require the integration of the CSMS ground events resource availability schedule with the SDPS production schedule. The segments would be able to share a database.

A final risk review and assessment by the ECS Project RMP will be completed by Release B, IDR. Trade-Off Studies Analysis Data for the ECS, 211-CD-001-001, February 1995, paragraph 6.26 details additional production planning and scheduling risk mitigation plans.

7.10.4 Contingency Plans

Production planning and scheduling risk contingency plans include providing the planning and scheduling activities manually.

7.11 Database Management Systems, (T-7)

7.11.1 Risk Description

DBMS risks include the potential for a single DBMS to fail to meet the ECS functional and performance requirements for spatial, temporal, and coincident search. A distributed database system was suggested, in which a collection of databases is logically related but physically distributed on multiple, cooperating nodes, each containing a set of usually non-disjointed data items. The benefits of a distributed database system are: location transparency, site autonomy, distributed query processing, increased response time, and distributed transaction processing.

7.11.2 Evaluation Criteria

DBMS evaluation criteria include:

a. Meeting query performance requirements.

b. Establishing the service interface.

c. Partitioning.

d. Data replicating.
e. Managing logically related databases.

Additional, the DBMS must meet the following criteria for distributed systems:

a. Location transparency.
b. Site autonomy.
c. Distributed query processing.
d. Fast response time.
e. Distributed transaction processing.

The DBMS system development evaluation must be completed and the risks must be mitigated by the IDR for the Release B design.

7.11.3 Risk Mitigation Plans

DBMS risk mitigation plans include studies and prototypes to resolve database management capability concerns. For example, the CSMS must conduct a study to determine whether the DBMS server should be installed at the management workstation to offload the system-level monitoring and local management servers, or the management workstation should use the DBMS server physically located on the Management Service System (MSS) enterprise monitoring and local management servers. Additionally, the plan includes the following studies and prototypes:

a. Data server architecture study.
b. Data type server prototype.
c. DBMS COTS encapsulation prototype.
d. Local Information Manager (LIM) prototype.

A final risk review and assessment by the ECS Project RMP will be completed by Release B, IDR. Trade-Off Studies Analysis Data for the ECS, 211-CD-001-001, February 1995 paragraph 6.32 details additional risk mitigation plans for data server architecture.

7.11.4 Contingency Plans

DBMS risk contingency plans include using a non-distributed database management strategy.

7.12 Processing and Storing Standard Products, (U-4)

7.12.1 Risk Description

The risk associated with processing and storing standard products is that the growth in science algorithms may exceed processing and storage resources. An accurate understanding of science algorithms is required to size data processing subsystem resources. Issues include:

a. Insufficient understanding of current resource assumptions and future growth trends exists.
b. The architecture and systems design may not scale to meet future requirements.
c. Not all products can be produced within the current budget (i.e., funds are the deficient resource).

Current projections of an expandable architecture reflect a processing growth factor of 8, and a data volume growth factor of 2. Currently, the design is considered “do-able,” but it exceeds all cost projections and expectations.

7.12.2 Evaluation Criteria

Evaluation criteria for processing and storing standard products include:

a. Processing and storage requirements must not exceed available resources.

b. Read/write stations and material handling must be increased.

c. The storage system must use optical tape in a 3480 form factor.

d. ECS must be able to interact with internal and external systems.

e. Stored data must be reorganized to improve retrieval performance.

The processing and storing standard products push side risk evaluation must be completed and the risks must be mitigated by the IDR for Release B.

7.12.3 Risk Mitigation Plans

Risk mitigation plans for processing and storing standard products include working with algorithm developers to refine performance models, designing for scalability over the Investigator Working Group (IWG) list, conducting prototypes to investigate alternative algorithm architectures, and continuing to use the PGS toolkit for development. These activities include:

a. Performance modeling.

b. Designing a scalable system with 8x processing and 2x storage of the IWG list.

c. Distributed and parallel computing science algorithm prototyping.

d. Science software execution prototyping.

e. Data processing prototyping.

f. PGS toolkit development and use.

A final risk review and assessment by the ECS Project RMP will be completed by Release B, IDR.

7.12.4 Contingency Plans

Contingency plans for processing and storing standard products include:

a. Using helical scan magnetic tape in place of optical tape. Storage media selection may potentially impact the floor space configuration [i.e., it depends upon having an approximate 50 Gigabyte (Gbyte)/tape using a 3480-D3 form factor].

b. Evaluating parallel processing capabilities.

c. Monitoring processing and storage technologies.

This page intentionally left blank.

8. Risk Control and Monitoring

This section links the high-risk items defined in Section 7 to milestones in the ECS development project. These milestones represent planned risk resolution dates. Paragraphs 8.1 and 8.2 describe the transition from understanding risks to resolving them as a two-step process.

8.1 Key Strategic Decisions

Identification of the decisions influenced by high risk is vital to transitioning from risk evaluation to risk planning. Key strategic decisions (see Figure 8-1) require significant preparation. Mitigation plans will be linked to these decisions. The key strategic decisions may be described as follows:

a. Decision 1—Functionality for Releases. User expectations must be met by matching the functionality required for each Release with the development organizations' capabilities.

b. Decision 2—DCE/CORBA Migration Plan. This is a series of decisions associated with migrating a COTS and standards-based infrastructure from DCE for Release A to OMG CORBA and object services for Release B.

c. Decision 3—Media and Form Factor for Archive. The media and form factor chosen for PB storage are critical. Cost and floor space requirements must be satisfied. This choice must include an evolution plan from the archive required for Release A. For example, maintaining the form factor would allow robotics reuse while upgrading media for higher density storage.

d. Decision 4—Design for Pull Side Performance. The implications of a potentially large number of non-science users accessing the ECS through a variety of service providers and requesting high volumes of electronic data distribution raise the criticality of performance-related decisions affecting these pull side users. These decisions include resource sizing, defining scalable designs, and selecting DBMS technologies.

e. Decision 5—Resources for Ante Meridiem-1 (AM-1) Satellite Algorithms. Understanding current resource assumptions, data dependencies, and future growth trends for standard product processing and storage is key to choosing the amount and design of data processing resources to be available for Release B.

8.2 Integrated Risk Mitigation Plan

Figure 8-2 shows key strategic decisions just prior to appropriate program milestones. A timeframe encompassing Releases A and B was chosen as critical for these decisions.

Decision 1 involves specifying the functionality per Release in the Release Plan. This was done for the SDR and will be shown in the next presentation. The Release Plan will be revisited for the Release B RIR.

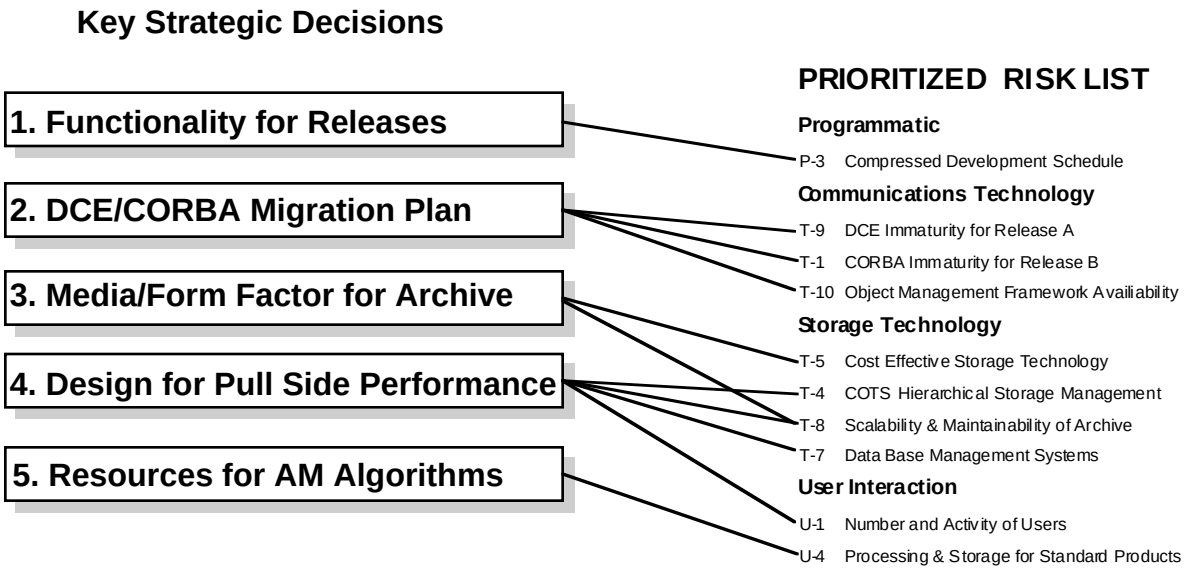

Figure 8-1. Key Strategic Decisions Mapped to the Prioritized Risk List

Decision 2's migration plan involves reviewing the technology insertion plans for DCE and CORBA and, if necessary, implementing contingency plans. For example, if a CORBA product is unavailable at the Release B IDR, development of a custom ORB over DCE will be initiated.

For the Release A PDR, archive technology must be chosen to satisfy TRMM requirements and be evolvable for later Releases. At the Release B IDR, the form factor and media must be chosen for the large AM archives.

Decisions 4 and 5, the push and pull decisions, involve two choices. First, the subsystem design scalability choices will be made for the Release B IDR. Second, the final sizing choices based on the latest modeling data will be made just prior to the Final Purchase Order date for Release B. These decision milestones are the basis for timing mitigation activities.

Based on the prioritized risk list, associated mitigation activities, and the key strategic decisions, an integrated risk mitigation plan has been developed (see Figure 8-3). This plan identifies completion dates for prototypes, studies, surveys and other mitigation activities supporting the decisions. This plan will be refined and implemented by the RMP. The plan will be refined, based on mitigation activity results, by changing the prioritized risk list. The plan will be implemented by making the strategic decisions and, if necessary, implementing contingency plans.

8.3 Risk Monitoring Parameters

Refer to Section 7 for individual monitoring parameters.

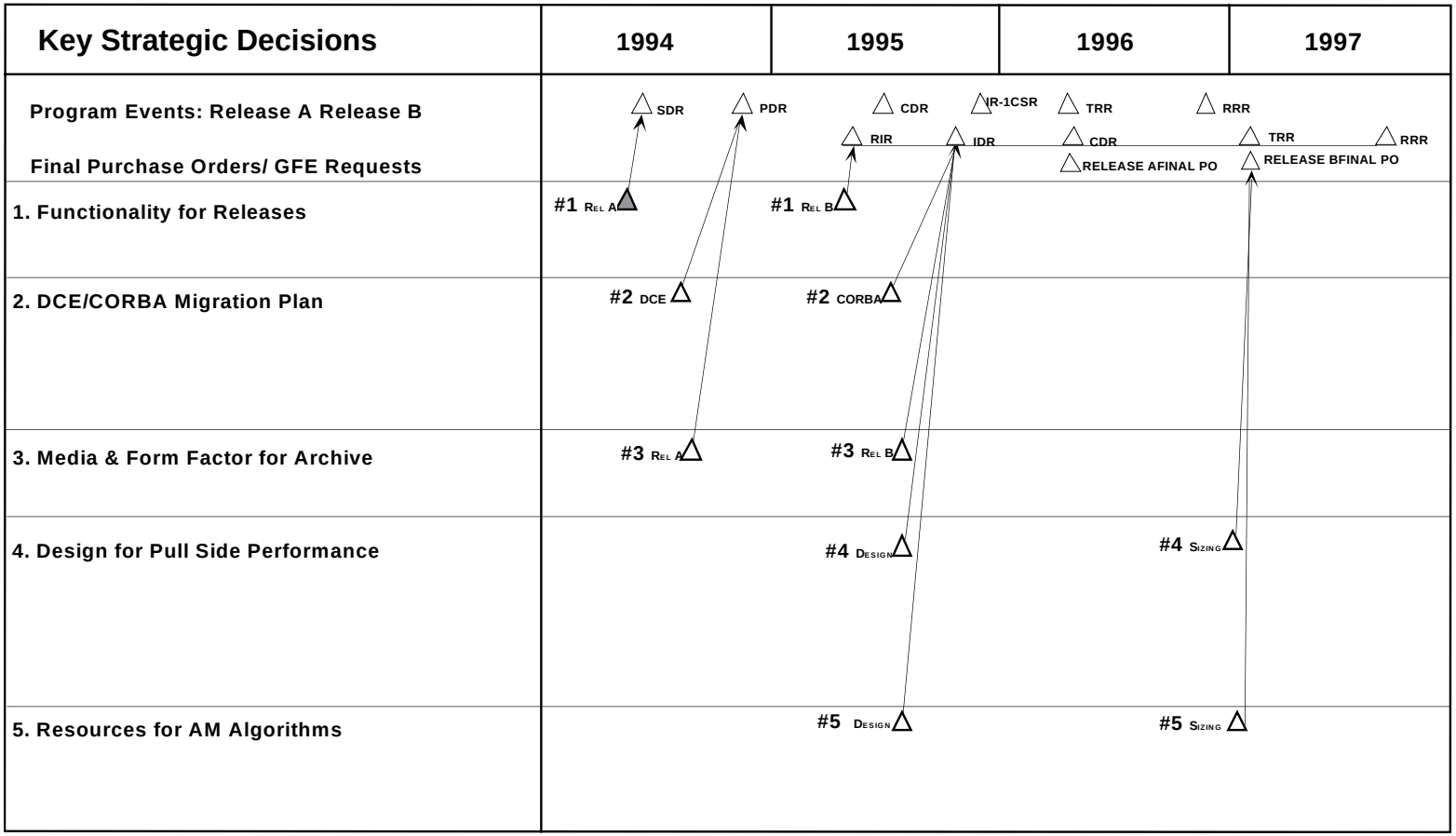

Figure 8-2. Key Strategic Decisions Linked to Program Milestones

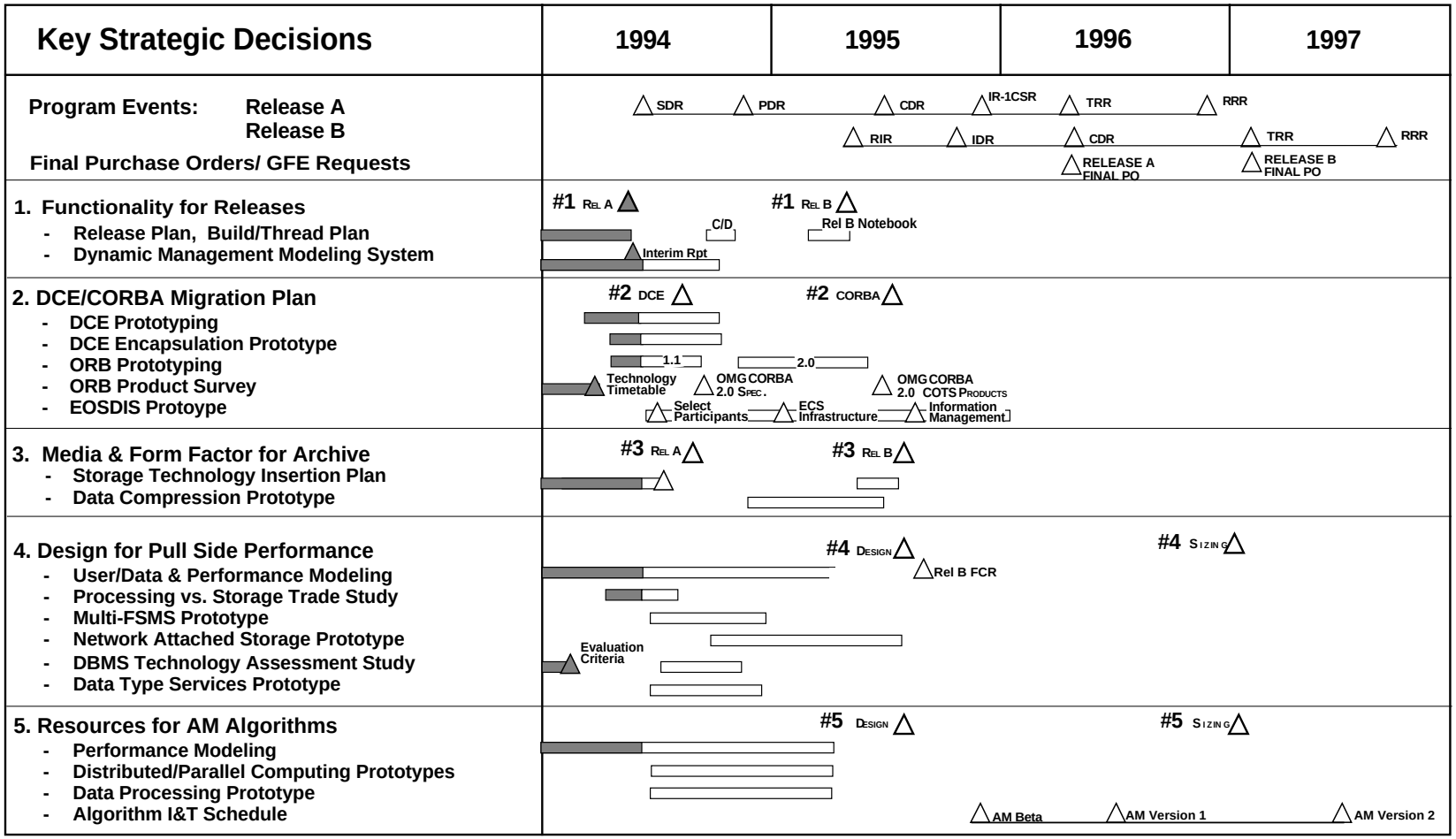

Figure 8-3. Integrated Risk Mitigation Plan

9. Interim Release 1 and Release A

This report specifically addresses the risk assessments for IR1 and Release A. The report identifies the risks and the activities and key decisions required to reduce these risks to acceptable levels.

9.1 Conclusions

The established RMP process and the policy instructions governing the process are effective in mitigating ECS risks. The policy instructions, program reviews, and RIDs resulting from the reviews acknowledge issues deserving detailed investigation to discover potentially hidden risks.

The effective risk mitigation approach has enabled management to make informed program development decisions. The mitigation process, as an ongoing activity, has been effective. Its anticipated results should compliment the ECS throughout the project lifecycle.

EPs and Release planning help to effectively evaluate and implement fielded, IR1, and Release A products.

The obvious conclusion to this report is to monitor the risks identified in Section 7 for IR1 and Release A, and to implement the processes defined in Section 8. There are, however, other activities supporting ECS risk management. ECS must to continue to evaluate evolutionary trends in the standards. These trends affect communications, ingest, processing, data storage and distribution, and control systems. Changes to the standards represent potential obstacles to ECS systems evolution.

9.2 Recommendations

The recommendations for IR1 and Release A are as follows:

a. Monitor the RID process for potential programmatic risks.

b. Continue RMP reviews in accordance with ECS policy instructions.

c. Continue to reassess and prioritize risks.

d. Monitor the progress of each programmatic risk.

e. Assess the effectiveness of risk management decisions using EPs, system performance, and requirements compliance.

This page intentionally left blank.

Abbreviations and Acronyms

3GL	Third Generation Language
4GL	Fourth Generation Language
AIS	Automated Information Security
AM-1	Ante Meridiem-1
ANSI	American National Standards Institute
API	Application Protocol Interface
ASTER	Advanced Spaceborne Thermal Emission and Reflection Radiometer
ATL	Automated Tape Library
BONeS	Block-Oriented Network Simulator
CASE	Computer-Aided Software Engineering
CCB	Configuration Control Board
CCR	Configuration Change Request
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CERN	European Laboratory for Particle Physics
CI	Contract Item
CORBA	Common Object Request Broker Architecture
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-The-Shelf
CSMS	Communications and System Management Segment
CSR	Consent to Ship Review
CSS	Communications Service System
DAAC	Distributed Active Archive Center
DADS	Data Archive and Distribution System
DBMS	Database Management System
DCE	Distributed Communication Environment
DEC	Digital Electric Corporation
DFD	Data Flow Diagram

DFS	Distributed File System
DID	Data Item Description
DME	Distributed Management Environment
DMR	Detailed Mission Requirements
DoD	Department of Defense
DPM	Deputy Project Manager
ECP	Engineering Change Process
EDF	ECS Development Facility
EDOS	EOS Data and Operations System
ECS	EOSDIS Core System
EOC	EOS Operations Center
EOS	Earth Observing System
EOSDIS	Earth Observing System Data and Information System
EP	Evaluation Package
ES	Earth Science
ESDIS	Earth Science Data and Information System
ESN	EOSDIS Science Network
ESUS	ECS Scientist User Survey
FIPS	Federal Information Processing Standard
FORTRAN	Formula Translation
FOS	Flight Operations Segment
FSMS	File and Storage Management System
GATT	Government Acceptance Test Team
Gbyte	Gigabyte
GCDIS	Global Change Data and Information System
GFE	Government-Furnished Equipment
GFI	Government-Furnished Information
GMU	George Mason University
GOSIP	Government Open System Interconnect Profile
GSFC	Goddard Space Flight Center
HDF	Hierarchical Data Format

HP	Hewlett Packard
HSM	Hierarchical Storage Management
I/F	Interface
I/O	Input/Output
I&T	Integration and Testing
IATO	Independent Acceptance Test Organization
ICC	Instrument Control Center
ICD	Interface Control Document
ICWG	Interface Control Working Group
IDL	Interactive Data Language
IDR	Incremental Design Review
IEEE	Institute of Electrical and Electronic Engineers
IMS	Information Management System
IP	International Partner
IPA	Inter-Project Agreement
IR1	Interim Release 1
IR&D	Independent Research and Development
IRD	Interface Requirements Document
IST	Instrument Support Terminal
IV&V	Independent Verification and Validation
IWG	Investigator Working Group
K	Thousand
KSLOC	Thousand Single Lines of Code
LAN	Local Area Network
LIM	Local Information Manager
LOC	Lines of Code
LOC/mm	Lines of Code per man month
Landsat	Land Satellite
M	Million
MIL-HDBK	Military Handbook
MIL-STD	Military Standard

MOU	Memorandum of Understanding
MSS	Management Service System
NASA	National Aeronautics and Space Administration
Nascom	NASA Communications
NCSL	National Computer Systems Laboratory
NFS	Network File System
NHB	NASA Handbook
NMI	NASA Management Instruction
NSI	NASA Science Internet
O&M	Operations and Maintenance
ODMS	Object Data Management System
OMB	Office of Management and Budget
OMF	Object Management Framework
OMG	Object Management Group
OODBMS	Object-Oriented Database Management System
OODCE	Object-Oriented Distributed Communication Environment
ORB	Object Request Broker
ORDBMS	Object Request Database Management System
PB	Petabyte
PDMP	Project Data Management Plan
PDR	Preliminary Design Review
PGS	Product Generation System
PI	Project Instruction; Principal Investigator
PIP	Project Implementation Plan
PM	Program Management
PO	Purchase Order
POSIX	Portable Operating System Interface for Computer Environments
PUB	Publication
RDBMS	Relational Database Management System
RID	Review Item Description
RIR	Release Initiation Review
RMA	Reliability, Maintainability, and Availability

RMP	Risk Management Panel
ROM	Read-Only Memory
RPC	Remote Procedure Call
RRR	Release Readiness Review
RTM	Requirements and Traceability Management
SCF	Science Computing Facility
SDPS	Science Data Processing Segment
SDR	System Design Review
SEER	System Evaluation and Estimate of Resources
SEM	System Element Management
SI&P	System Integration and Planning
SLOC	Single Lines of Code
SMC	System Monitoring and Control
SOFT	Software Operations Focus Team
SRR	System Requirements Review
STD	Standard
STK	Storage Tek
STL	Science and Technology Laboratory
StP	Software Through Pictures
StP/OMT	Software Through Pictures/Object Modeling Technique
TB	Terabyte
TBD	To Be Determined
TBR	To Be Resolved
TL	Team Leader
TRMM	Tropical Rainfall Measurement Mission
TRR	Test Readiness Review
UCB	University of California, Berkeley
UND	University of North Dakota
UserDIS	User Data Information System
WAN	Wide Area Network
WBS	Work Breakdown Structure

This page intentionally left blank.